



AndroidPIT



Andreas Itzchak Rehberg

Das inoffizielle

Android System-Handbuch

- Benutzen Sie die besten Tools zur System-Pflege
- Erlangen Sie tiefe Einblicke ins Android-System
- Sorgen Sie für Sicherheit auf Ihrem Android-Gerät

Dem Android-System unter die Haube geschaut!
In Zusammenarbeit mit AndroidPIT, der größten
deutschsprachigen Community zu Android.

FRANZIS

Andreas Itzchak Rehberg

**Das inoffizielle Android
System-Handbuch**

Andreas Itzchak Rehberg

Das inoffizielle

Android System-Handbuch

- Benutzen Sie die besten Tools zur System-Pflege
- Erlangen Sie tiefe Einblicke ins Android-System
- Sorgen Sie für Sicherheit auf Ihrem Android-Gerät

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Alle Angaben in diesem Buch wurden vom Autor mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. Der Verlag und der Autor sehen sich deshalb gezwungen, darauf hinzuweisen, dass sie weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen können. Für die Mitteilung etwaiger Fehler sind Verlag und Autor jederzeit dankbar. Internetadressen oder Versionsnummern stellen den bei Redaktionsschluss verfügbaren Informationsstand dar. Verlag und Autor übernehmen keinerlei Verantwortung oder Haftung für Veränderungen, die sich aus nicht von ihnen zu vertretenden Umständen ergeben. Evtl. beigefügte oder zum Download angebotene Dateien und Informationen dienen ausschließlich der nicht gewerblichen Nutzung. Eine gewerbliche Nutzung ist nur mit Zustimmung des Lizenzinhabers möglich.

© 2012 Franzis Verlag GmbH, 85540 Haar bei München

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Das Erstellen und Verbreiten von Kopien auf Papier, auf Datenträgern oder im Internet, insbesondere als PDF, ist nur mit ausdrücklicher Genehmigung des Verlags gestattet und wird widrigenfalls strafrechtlich verfolgt.

Die meisten Produktbezeichnungen von Hard- und Software sowie Firmennamen und Firmenlogos, die in diesem Werk genannt werden, sind in der Regel gleichzeitig auch eingetragene Warenzeichen und sollten als solche betrachtet werden. Der Verlag folgt bei den Produktbezeichnungen im Wesentlichen den Schreibweisen der Hersteller.

Herausgeber: Anton Schmid

Satz: www.buch-macher.de

art & design: www.ideehoch2.de

Druck: C.H. Beck, Nördlingen

Printed in Germany

ISBN 978-3-645-60215-0

Vorwort

Mein erstes Android-Buch, *Das inoffizielle Android-Handbuch*, erfreut sich nach wie vor großer Beliebtheit, und bereits nach wenigen Monaten war eine Neuauflage notwendig: Der Vorrat im Lager des Verlags war aufgebraucht! Was bleibt mir bei derart großem Interesse anderes übrig, als für eine Fortsetzung zu sorgen?

Was diese zum Thema hat, lässt sich bereits am Namen erkennen: Das Android-System selbst. Es wird insbesondere auf die Konfiguration eingegangen – ebenso aber auch auf Themen wie Backup und Datensicherheit. Wie gewohnt, werden natürlich Werkzeuge (Apps) benannt, mit denen sich das System im Griff behalten lässt, mit denen man es also konfiguriert und ggf. auch repariert. Neben all diesen Apps sollen aber Praxis-Tipps und Hintergründe auch nicht fehlen.

Wo sich all diese (und weitere) Werkzeuge finden lassen? Überwiegend natürlich wieder in meinen *App Reviews nach Einsatzzweck* bei *AndroidPIT*, deshalb wird auch an mancher Stelle für mehr Details oder für weitere Apps zu einem Themenbereich dorthin verwiesen. Im Forum findet sich dann auch wieder ein Thread für Fragen und Anregungen.

Anders als im *inoffiziellen Android-Handbuch* geht es in diesem Band um mehr als nur einen kurzen Überblick – hier wird tiefer eingestiegen. Dennoch finden sich auch wieder Verweise zu den entsprechenden Themen im Forum, nicht unbedingt zur Vertiefung, aber dort sind die Informationen oft aktueller und vollständiger.

Und noch eins muss ich loswerden: Viele der hier kurz vorgestellten (oder auch nur genannten) Apps habe ich selbst nie getestet – dafür fehlt einfach die Zeit: Würde ich jede App erst selbst testen, wäre ich noch immer mit dem ersten Buch beschäftigt. Und wäre das dann fertig, könnte ich gleich wieder von vorn beginnen – einfach weil die Informationen bis dahin bereits veraltet wären. Ein Grund mehr, auf die Erfahrungen der Community zurückzugreifen: Bei AndroidPIT ist jeder jederzeit herzlich willkommen! Auch für Feedback sowie Fragen zu diesem Buch findet sich dort ein Plätzchen.



<http://www.androidpit.de/de/android/forum/thread/409715/>



<http://www.androidpit.de/>

Hinweise zur Nutzung des Buches

Wie bereits im Vorwort aufgeführt, handelt es sich bei diesem Buch um eine Fortsetzung meines Buches *Das inoffizielle Android-Handbuch*. Ausgewählte Themen sollen hier vertieft werden. Teilweise setze ich Kenntnisse voraus, die im „ersten Band“ behandelt wurden.

Auch wenn die Themen hier ausführlicher behandelt werden, so finden dennoch nicht alle verfügbaren Apps Erwähnung. Das ist auch gar nicht möglich. Nicht nur würde es den Umfang dieses Buches sprengen – es wäre auch schon nicht mehr aktuell, kaum dass es die Buchläden erreicht hätte: Täglich finden hunderte oder gar tausende neue Apps ihren Weg in den Google Playstore. Daher stehen auch die in diesem Buch vorgestellten Apps exemplarisch für die Möglichkeiten, die Android im jeweiligen Zusammenhang bietet. Weitere Apps sind in der Regel im zu Beginn eines Kapitels genannten Forums-Thread zu finden, ebenso wie Kommentare ihrer Nutzer.

Ein weiterer Hinweis gilt den Screenshots: Diese sind oft der Playstore-Seite der jeweiligen App entnommen und daher häufig auf Englisch. Das muss allerdings nicht zwangsläufig heißen, dass selbige App dann nicht auch auf Deutsch läuft – meist ist das der Fall. Es belegt also lediglich, dass sie auch Englisch kann ...

Einige der hier vorgestellten Tools und Apps setzen den root-Zugang (vgl. Abschnitt 2.1) zum Gerät voraus. Stellen, an denen solche Anwendungen beschrieben werden, sind am Seitenrand mit einem Symbol und einem grauen Balken markiert.

Danksagung

Auch diese gehört an den Anfang eines guten Buches. Ich füge sie hier jedoch nicht aus reinem Pflichtbewusstsein ein – sondern weil ich einigen Menschen auch und gerade in Zusammenhang mit diesem Buch wirklich dankbar bin.

Meine liebe Frau möchte ich dieses Mal gleich an erster Stelle nennen: Wiederum fand sie mich über Wochen und Monate hinweg fast nur an der Tastatur vor. Wahrscheinlich sucht sie auch bereits nach einer Möglichkeit, bei ihrem Mann einen „Factory-Reset“ durchzuführen oder ein passendes Custom-ROM aufzuspielen (um das Verhalten anzupassen). Danke für Dein großes Herz und Verständnis!

Zu einigen Details hat mich Andrew Hoogs Buch „Android Forensics“ inspiriert, das ich dankenswerterweise für den Franzis Verlag übersetzen durfte (es ist mittlerweile unter dem Titel „Android Forensik“ auch in deutscher Sprache verfügbar). Andrew und seinem Team, insbesondere auch Kevin, an dieser Stelle meinen besonderen Dank – nicht nur für die Inspiration, sondern auch für den interessanten und fruchtbaren Austausch per Mail zu diversen Details.

Toni, meinem Lektor bei Franzis, sei an dieser Stelle ebenfalls gedankt: Er hat schließlich die Sache mit Andrews Buch eingefädelt. Und mir auch erlaubt, mich für „Das inoffizielle Android-Systemhandbuch“ an den dortigen Themen zu bedienen. Einige kurze Passagen meiner Übersetzung sind daher auch hier eingeflossen.

Weitere dankbare Grüße gelten den Communities bei *AndroidPIT* und *StackExchange* – insbesondere Zuul, t0mm13b, ce4 und Flow. Von Euch habe ich zahlreiche Anregungen erhalten, mit Euch meine Ideen diskutiert (dabei so manche Nacht im Chat verbracht) und viel dabei gelernt. Das sollten wir auf jeden Fall fortsetzen!

Abschließend noch meinen Dank an die Leser dieses Buches, die nun schon bis hierher durchgehalten haben, hoffentlich auch noch ein wenig weiter lesen und aus diesem Buch möglichst großen Nutzen ziehen: Viel Spaß bei der Lektüre – und mit Euren Androiden!

Inhaltsverzeichnis

1 Sicherheit	12
1.1 Safety	12
Lokale Backups	12
Backup in die Cloud	29
Synchronisation	33
1.2 Security	47
Verschlüsselung	47
Zugriffsrechte	61
Location-Cache	67
Malware und Viren	69
Diebstahlschutz	80
1.3 App-Sicherheit	84
Gespeicherte Daten	84
Übertragene Daten	89
Weitere Sicherheits-Probleme	91
2 System	93
2.1 Der Super-User „root“	93
Vorteile des root-Zugangs	94
Risiken des root-Zugangs	95
Wie bekomme ich root-Zugang?	95
Laufen dann alle Apps mit root-Rechten?	96
Gibt es irgendwo weitere Infos zu diesem Thema?	97
2.2 Dateisysteme und Datenstrukturen	99
Der Boot-Prozess	99
Dateisysteme	102
Datenstrukturen	110
2.3 System-Info	116
Systeminfo-Widgets	116
Schnellumschalter	119
Ausführlichere System-Infos	122
System Logs	125
Monitoring	133
2.4 Konfiguration	137
Konfiguration mit Bordmitteln	137
Ausgewählte bzw. häufig genutzte Einstellungen	151
Zusätzliche bzw. versteckte Einstellungen	153

2.5	Automatisierung	156
	Zeitschaltuhren.....	157
	Ortsbasiertes Schalten.....	158
	Zeit-, Orts- und eventbasiertes Schalten.....	159
	Tasker.....	161
2.6	Datei-Manager.....	164
	Für den „normalen Anwender“	164
	Spezielles für „Wurzelmenschen“ (root)	167
	Toolboxen mit integriertem Datei-Manager	169
2.7	Androiden vom PC aus verwalten.....	172
	Für den „normalen Anwender“	172
	Für den „Power-User“	176
2.8	Custom Recovery und ROMs	178
	Custom Recovery: ClockworkMod.....	178
	Nandroid-Backups	180
	Stock ROMs und AOSP	182
	Custom-ROMs.....	184
	CyanogenMod.....	185
3	Netzwerk	187
3.1	Netzwerk-Konfiguration.....	187
	An und Aus	187
	Datensynchronisation im Hintergrund	189
	WLAN-Konfiguration.....	189
3.2	Administration	191
	Geräte-Informationen abfragen	191
	Diagnose: Was geht schief?.....	193
	Remote-Laufwerke mounten	202
3.3	Sichere Übertragung.....	204
	Proxy, Tunnel & Co	204
	AdBlock.....	208
3.4	WLAN	211
	VPN	211
	Automatische (De-)Aktivierung.....	213
	Tethering	217
	Reverse Tether	220
	Hotspots & WLAN-Finder.....	222
	War-Driving.....	228
3.5	Dienste bereitstellen	230
	Kabelgebunden	230
	Kabellos	233

4 Tuning	245
4.1 Einleitung und Überblick	245
Generelle Maßnahmen	245
Bessere Akku-Laufzeit	246
Mehr Speed	246
4.2 Generelle Tuning-Maßnahmen	247
Nicht mehr verwendete/benötigte Apps deinstallieren	247
Cache bereinigen	249
Selten genutzte Apps am automatischen Starten hindern	251
Das Märchen vom Task-Killer	255
4.3 Längere Akkulaufzeiten erreichen	256
Deaktivierung ungenutzter Dienste	257
Display-Einstellungen	258
Hintergrunddaten und Synchronisierung	259
Verschiedenes	260
Akku-Pflege	261
CPU untertakten	264
Kleine Helferlein	265
4.4 Platz im internen Speicher schaffen	270
Aufräumen	270
Auslagern	271
4.5 Need For Speed	272
RAM bereinigen	273
Swap-Space nutzen	275
CPU übertakten	276
 A Anhang	 278
A.1 Fragen und Antworten	278
Apps & Co.	278
Backup & Co.	281
Rund um die SD-Karte	286
Tuning	288
Verschiedenes	293
A.2 Begriffserklärungen	294
A.3 Google Permissions – und was sie bedeuten	309
A.4 Akkuverbrauch im Mobilfunk-Standby mit Tasker bekämpfen	319
A.5 Diebstahl-Schutz mit Tasker	325
A.6 Secret Codes oder Magische Nummern	326
A.7 Leistungsaufnahme verschiedener Komponenten	329
 Stichwortverzeichnis	 332

1 Sicherheit

Leider haben wir im Deutschen wohl nur das eine Wort – wo andere Sprachen, wie etwa das Englische, durchaus zwischen verschiedenen Arten von Sicherheit zu unterscheiden wissen.

Es gilt bei dem Wort „Sicherheit“ sehr wohl zu unterscheiden, was man denn nun eigentlich meint. Und was ich hier meine, wenn ich diese Begriffe in die Tastatur hacke, soll folgende Grafik veranschaulichen – die damit gleich nebenbei die Struktur dieses Kapitels abbildet:

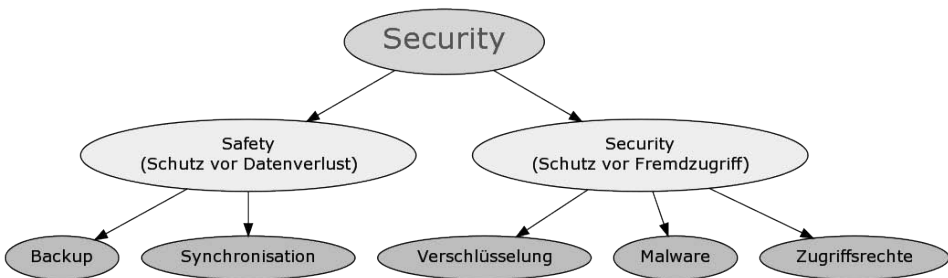


Bild 1.1: Der Begriff „Sicherheit“ lässt sich in verschiedene Bereiche unterteilen

1.1 Safety

Mit „Safety“ meine ich: Schutz vor Datenverlust. Schützt nicht vor dem Verlust des Androiden selbst: Genügend „Kleingeld“ vorausgesetzt, lässt sich dieser noch relativ einfach ersetzen. Doch die persönlichen Daten, die gibt es nicht im Laden: Termine, Adressen, Fotos, ... Wo bekommt man die wieder her, wenn die aus „Spaceballs“ bekannte Ansage provoziert wurde: „Vielen Dank, dass Sie den Selbstzerstörungsmechanismus aktiviert haben ... 3...2...1...Tschüss!“?

Lokale Backups

Ah, aus dem Backup? Werfen wir zunächst einen Blick in „Murphys Gesetze“. Da heißt es unter anderem:

Backup: Etwas, das man nicht braucht, wenn man es hat – oder nicht hat, wenn man es braucht. Hat man es, wenn man es braucht, ist es entweder nicht lesbar – oder zumindest der Sektor mit der wichtigsten Datei kaputt.

Damit einem dieses Schicksal erspart bleibt, kann man mit Netz, doppeltem Boden und Sicherheitsleine arbeiten: Ein Backup auf der SD-Karte, eine Kopie davon auf dem PC und eine weitere außerhalb der eigenen vier Wände. Vielleicht nicht unbedingt im Bank-Tresor, aber auf einem fremden Server sollte es dann auch verschlüsselt sein. Nicht nur, um es vor unbefugten (Ein-)Blicken, sondern auch vor etwaiger Fremd-Modifikation zu schützen. Wie weit man das Ganze treibt, bleibt natürlich jedem selbst überlassen.

Die nötigen Werkzeuge werde ich jedoch hier nennen. Ich muss dabei zugeben, dass ich in Sachen Datenschutz vielleicht ein wenig paranoid bin: So bevorzuge ich Lösungen, die ohne Netzwerk-Permissions auskommen. Sollen die Daten dann doch irgendwo außerhalb meines Androiden abgelegt werden, lasse ich das lieber von einer separaten App erledigen. Dieser Sachverhalt wird sich hier wohl widerspiegeln.

Natürlich werde ich an dieser Stelle nicht auf alle verfügbaren Apps eingehen – dafür sind es einfach zu viele. Eine entsprechende Übersicht findet sich jedoch im **Forum**.



[www.androidpit.de/
de/android/forum/
thread/412710/](http://www.androidpit.de/android/forum/thread/412710/)

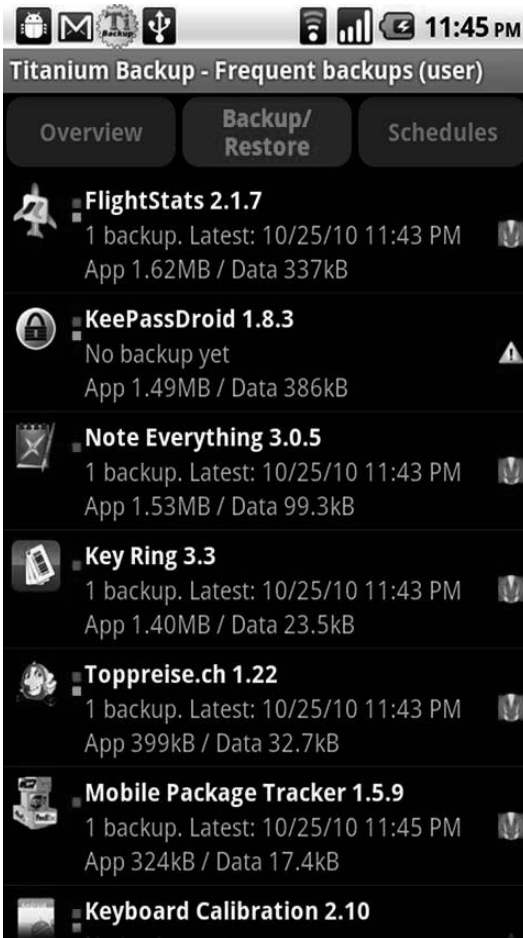
Komplettsicherungen

Titanium Backup

Fragt man nach einer guten Backup-App, taucht zweifellos **Titanium Backup** (Bild 1.2) bei den Antworten auf. Aus meiner Sicht ist dies die wirklich beste Lösung, sie hat nur einen Haken: Man benötigt dafür root-Rechte. Bei genauerem Nachdenken ist das logisch – wie sonst will man wirklich überall rankommen? Und **Titanium Backup** kann wirklich alles sichern, System-Apps eingeschlossen. Letztere lassen sich damit sogar „einfrieren“ oder, für ganz Harte, vollständig entfernen: So wird man die ganzen „Zwangsbeglückungen“ los, die einem Hersteller (und, bei Geräten mit Branding, auch die Provider) auf's Auge drücken – die aber kaum jemand braucht.

Die Erläuterung aller Features dieser App würde beinahe für ein eigenes Buch ausreichen, also muss ich mich auf das Wesentlichste beschränken. Ein vollständiges Backup einschließlich aller Apps und ihrer Daten bedarf eigentlich keiner gesonderten Erwähnung – das kann man mit Fug und Recht erwarten (sonst wäre es ja kein Komplett-Backup; die Sicherung erfolgt übrigens wahlweise auf SD-Karte oder auch in die Dropbox). Gleiches gilt für die Wiederherstellung – denn was nützt ein Backup ohne diese Möglichkeit? Aber die zahlreichen Kleinigkeiten sind es, die **Titanium Backup** so einzigartig machen.





Titanium Backup

Bild 1.2: *Titanium Backup* ist die bekannteste und beliebteste Lösung für Komplett-Backups – erfordert allerdings root-Rechte

So lässt sich festlegen, wie viele „Generationen“ man denn aufheben möchte, damit man bei Bedarf auch auf eine ältere Sicherung zurückgreifen kann. Eingangs erwähntem „Murphy“ zufolge stellt man einen Fehler nämlich erst dann fest, wenn er schon ins Backup übernommen wurde. Oder der Market-Doktor: Taucht eine App im Playstore nicht mehr unter den eigenen Apps auf? Kein Thema: Der Market-Doktor repariert das. Hat ein Update eine App unbrauchbar gemacht? Na, dann holen wir uns aus einer „vorigen Generation“ eine ältere Version zurück. Versehentlich in einer App zu viele Daten gelöscht? Die sind im Backup ebenfalls enthalten. Das Gerät wird immer langsamer? Dann lassen wir doch mal den Dalvik-Cache ein wenig aufräumen.

Und da wir ja alle ein wenig vergesslich sind – aber dennoch im Notfall gern ein aktuelles Backup hätten: Mit *Titanium Backup* lassen sich auch automatische Backups erstellen ...



Für weitere Details etwa bezüglich Dropbox-Support, der Nutzung von Labeln, dem Wiederherstellen von Backups nach einem Systemupdate oder gar dem Übertragen der Datensicherung auf ein neues Gerät empfiehlt sich ein Besuch auf der *Homepage*. Dort steht u. a. auch ein hilfreiches Wiki bereit.

Nandroid Backup

Eine weitere Art des Komplett-Backups führt über die sogenannte Recovery-Konsole – allerdings in der erweiterten Version, wie sie Custom-Recoveries bereitstellen. Am bekanntesten ist in diesem Umfeld ClockworkMod (kurz: CWM; Bild 1.3 zeigt einen Screenshot einer älteren Version) von Koushik Dutta, besser bekannt als „Koush“. Für *ClockworkMod* findet sich im Netz sogar ein (zwar leicht veralteter, aber dennoch sehr nützlicher) *englischsprachiger Guide*.

ClockworkMod Recovery v2.5.0.1

```
- reboot system now
- apply sdcard:update.zip
- wipe data/factory reset
- wipe cache partition
- install zip from sdcard
- nandroid
- partitions menu
- advanced
```

ClockworkMod Recovery v2.5.0.1



<http://www.matrixrewriter.com/android/>



<http://www.addictivetips.com/mobile/what-is-clockworkmod-recovery-and-how-to-use-it-on-android-complete-guide/>

Bild 1.3: *ClockworkMod Recovery* ist die bekannteste Recovery-Konsole

Anders als bei *Titanium Backup* werden hier keine einzelnen Dateien gesichert, sondern es wird ein Image der gesamten Partitionen angelegt. Für Windows-User lässt sich dies vielleicht mit Norton Ghost vergleichen – eingefleischten Linux-/Unix-Nutzern reichen als Beschreibung die beiden Buchstaben *dd*. Aus jeder Partition wird somit eine Datei auf der SD-Karte, die sich dann natürlich auch zur weiteren Sicherheit auf den Computer kopieren lässt.



Sinnvollerweise erstellt man in regelmäßigen Abständen – und insbesondere vor größeren Änderungen – eine solche Komplettsicherung, beispielsweise vor der Installation eines neuen ROM-Images. Geht dann etwas schief, lässt sich der „lauffähige Zustand“ recht einfach wieder herstellen, indem man die erstellten Images über das Recovery-Menü wieder herstellt.



AppExtractor



www.xda-developers.com/android/online-nandroid-backups-without-rebooting-porting-to-most-android-devices/

Und nun bringen wir die beiden genannten Kandidaten zusammen: Interessanterweise kann *Titanium Backup* nämlich auch einzelne Daten (etwa eine App inklusive ihrer Einstellungen) aus Nandroid-Backups wiederherstellen. Somit lassen sich ggf. kleinere „Fehler“ wieder korrigieren – wenn man etwa vor dem Einspielen eines neuen Custom-ROMs die Daten einer App zu sichern vergessen hat. Oder sich erinnert, dass ein älteres Nandroid-Backup noch etwas enthält, was man auf dem neuen Gerät nicht mehr hat – wobei übrigens alternativ auch der *AppExtractor* helfen kann.

Wer so ein Nandroid-Backup für eine interessante Sache hält, es aber als zu umständlich empfindet, dafür jedes Mal ins Recovery-Menü zu booten (da ist man ja offline! Man könnte eine wichtige Facebook-Meldung verpassen!), der sollte einmal bei den XDA-Developers vorbeischauchen. Dort hat nämlich jemand ein Tool gebastelt, welches Nandroid-Backups im laufenden Betrieb erstellt. Also so ganz ohne Booten und ohne Facebook-Ausfall ...

Komplett-Backups ohne root

Vom Androiden aus sind sie eigentlich unmöglich: Das Berechtigungs-System lässt es bekanntlich nicht zu, dass eine App auf die Daten einer anderen direkt zugreift, ohne dass letztere diese Daten explizit freigegeben hat – was in der Regel ja nicht der Fall ist. Wie aber will man ein solches auf anderem Wege erreichen?

Mit Android 4.0 (auch als *Ice Cream Sandwich* bekannt) wurde, nahezu undokumentiert, eine solche Möglichkeit geschaffen: Der auf dem Gerät laufende ADB-Daemon hat hier zusätzliche Rechte erhalten. Nutzen lassen sich diese für ein Backup allerdings nur, wenn auf einem per USB-Kabel angeschlossenen Computer auch ein entsprechender Client zur Verfügung steht. Dies trifft zu, sofern man das SDK dort installiert hat. Dann nämlich kann man den Befehl `adb backup` an der Kommandozeile absetzen:

```
adb backup [-f <file>] [-apk|-noapk] [-shared|-noshared] [-all]
[-system|nosystem] [<packages...>]
```

Die erwähnten Optionen stehen dabei für Folgendes:

- f – Pfad und Name der auf dem Computer abzulegenden *.ab-Datei. Bei dieser handelt es sich um eine komprimierte Archiv-Datei, welche die Apps und Daten des Android-Geräts enthält.
- apk | -noapk – gibt an, ob die *.apk-Dateien (Apps) mit verarbeitet werden sollen.

Default ist `-noapk`.

`-shared` | `-noshared` – Aktivieren/Deaktivieren des Backups von Inhalten des „externen Speichers“ („shared storage“, SD-Karte). Default ist hier `-noshared`.

`-all` – gibt an, dass das gesamte System gesichert werden soll (Komplett-Backup). Alternativ lassen sich mit dem Filter `<packages>` auch einzelne (oder mehrere) Apps sichern.

`-system` | `-nosystem` – spezifiziert, ob System-Apps (und ihre Daten) im Backup enthalten sein sollen. Default ist `-system`.

`<packages>` – hier lassen sich einzelne Pakete (Apps) zur Sicherung angeben, wenn kein Komplett-Backup erfolgen soll. Bei Verwendung der Option `-all` wird dies nicht benötigt.

Ein Beispiel-Aufruf könnte wie folgt aussehen:

```
adb backup -apk -shared -all -f ~/backup/Desire_2012-08-28.ab
```

Oder, für Windows-Anwender:

```
adb backup -apk -shared -all -f C:\backup08262012.ab
```

Auf dem Gerät löst dieser Befehl einen Hinweis aus, wie er in Bild 1.4 zu sehen ist. Der Cursor zeigt bereits an: Hier wird eine Benutzer-Eingabe erwartet. Und zwar soll das Passwort angegeben werden, mit dem das Backup sodann verschlüsselt wird; wir haben ja bereits gelernt: Das Wort „Sicherheit“ hat zwei Bedeutungen. Durch das eigentliche Backup existiert eine Kopie, die vor Datenverlust schützen soll – und durch die Verschlüsselung wird Unbefugten der Zugang zu diesen Daten erschwert.

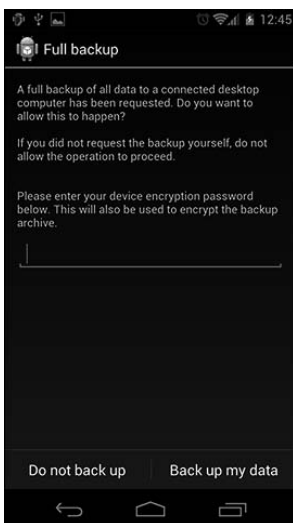


Bild 1.4: Nach Anstoß des Backups vom Computer erfolgt auf dem Android-Gerät diese Abfrage

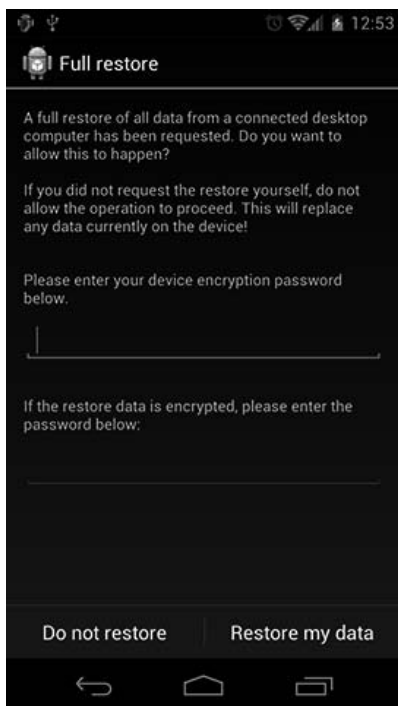


Bild 1.5: Dieser Bildschirm zeigt sich auf dem Android-Gerät nach Aufruf des Befehls zur Datenwiederherstellung

Analog geht es in der Gegenrichtung zu, wenn ein Backup wieder hergestellt werden soll:

```
adb restore ~/backup/Desire_2012-08-28.ab
```

Oder, für Windows-Anwender:

```
adb restore C:\backup08262012.ab
```

Auch hier erfolgt wieder die Abfrage des Passwortes (siehe Bild 1.5): Das Backup wurde ja verschlüsselt und muss somit zur Wiederherstellung auch entschlüsselt werden. Wer beim Wiederherstellungs-Befehl genauer hinschaut, hat es sicher bereits gesehen: Dieser kennt als einzigen Parameter die Datei des wiederherzustellenden Backups. Einzelne Daten lassen sich also scheinbar nicht aus einem vollständigen Backup direkt auf das Gerät zurücktransferieren.

Aber geht das wirklich nur über die Kommandozeile? Und von Hand? Die XDA-Developer haben sich da natürlich bereits etwas einfallen lassen, und so berichtet ein dortiger Artikel vom *Ultimate Backup Tool*, natürlich für Windows. Mittlererweile gibt es das Tool aber auch für den Mac, wo es jedoch ein installiertes SDK voraussetzt. Da es sich hier um ein Shell-Script handelt, sollte Linux-Fans eine Anpassung nicht schwer fallen.



<http://www.xda-developers.com/android/ultimate-backup-tool-no-root-required/>

Was aber tun diejenigen, die viel lieber die Maus schubsen würden? Ein klein wenig warten vielleicht. Denn Ryan Conrad (dem ich an dieser Stelle für den Hinweis auf diese Möglichkeit danken möchte) erweitert gerade seinen **Droid Explorer** (Bild 1.6). Ab Version 0.8.8.7 wird dieses Tool, das sich sonst hauptsächlich an „Wurzelmenschen“ richtet, dieses Backup auch für nicht-gerootete Geräte unterstützen. Weitere Tools, die dies unterstützen, sind übrigens auch in dem Abschnitt *Für den „Power-User“* in Kap 2.8 beschrieben.



Droid Explorer



Bild 1.6: **Droid Explorer** bietet ab Version 0.8.8.7 eine Schnittstelle zum ADB-Backup

Eine echte Alternative zu finden, die sich direkt auf dem Androiden ausführen lässt und dabei ebenfalls ohne *root* auskommt, scheint unmöglich. Nicht einmal wirklich nah heran kommt man da, wenn es etwas Gutes sein soll. Die Bewertungen sind bestenfalls ziemlich durchwachsen, wie auch die Erfahrungen der Benutzer.

MyBackup Pro (Bild 1.7) kommt in den Kommentaren noch recht gut weg (anders als die zugehörige Testversion). Die App soll ebenfalls ein komplettes Backup auf der SD-Karte anlegen und natürlich von dort wiederherstellen können. Explizit erwähnt wird auch die Möglichkeit, auf diese Weise die Daten auf einem anderen Gerät wieder einzuspielen.

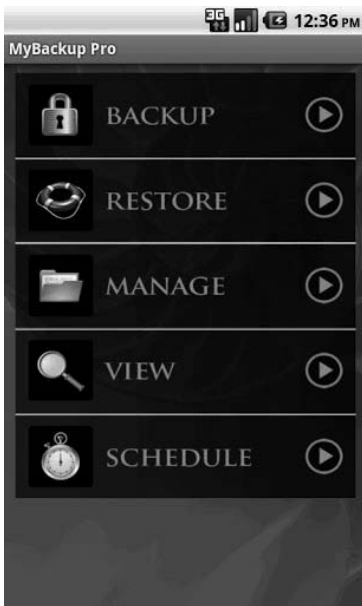


Bild 1.7: *MyBackup Pro* sichert die meisten Daten ohne root

Da die App die Backups auf den Online-Servern des Anbieters speichern möchte, ist ein entsprechender Vertrauensvorschuss nötig: Die Kombination aus Zugriff auf Internet *und* persönliche Daten ist immer ein wenig heikel. Der Preis für diese App liegt mit knapp vier Euro (eine Gratis-Testversion ist ebenfalls im Playstore verfügbar) leicht unter dem von *Titanium Backup*. Anwendern mit root-Zugriff würde ich dennoch eher Letzteres empfehlen.



Sprite Backup

Auch bei *Sprite Backup* ist die Liste der verlangten Berechtigungen lang (für eine Backup-App ja normal) und schließt neben dem Zugriff auf persönliche Daten wie Kontakte auch das Internet ein: Eine Datensicherung ist hier auf die SD-Karte, aber auch in die Dropbox oder bei Box.Net möglich. Also in die Cloud – und das geht nun einmal nicht ohne Internet. Laut Screenshots scheint hier zwar fast alles gesichert zu werden – doch die Kommentare sind, euphemistisch ausgedrückt, recht durchwachsen und lassen Zweifel an einer vollständigen Wieder-

herstellung aufkommen. Leider bietet die knapp vier Euro teure App keine Testversion, um sich selbst vor dem Kauf ein Bild machen zu können. In den 15 Minuten, die Google hier zum Test gewährt, ist ein solcher schlicht unmöglich.

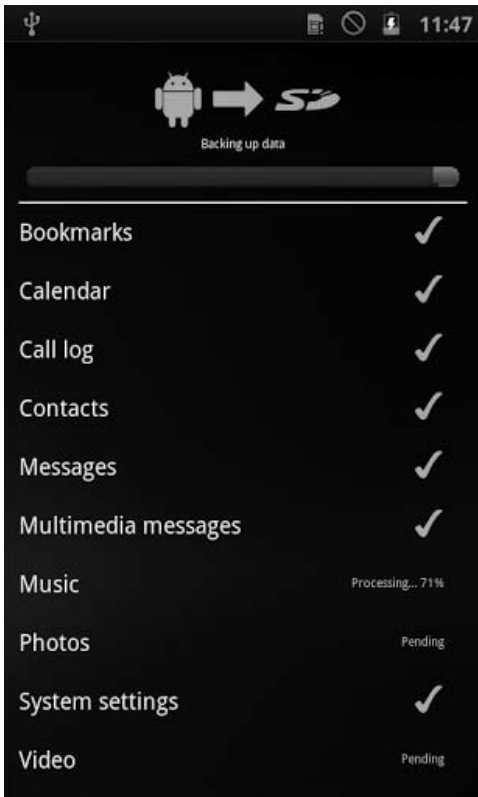


Bild 1.8: Auch **Sprite Backup** verspricht, vieles zu sichern

Und so erschöpfen sich die Alternativen auch schon – denn bei den anderen mir bekannten Nicht-root-Lösungen sieht es nicht besser aus. Bleibt als Fazit der Satz stehen: „Ohne *root* sich nichts tut“. Zumindest im Bereich der Komplettbackups.

Apps sichern

Dafür sieht es in diesem Bereich auch für Anwender ohne *root* recht gut aus – denn hier gibt es das **AppMonster**. Dieses schlägt in der Pro-Version mit knapp drei Euro zu Buche – hat mir aber nicht nur einmal den Tag gerettet.

Die Hauptfunktionalität dieser App besteht darin, bei jeder Neuinstallation automatisch eine Kopie der .apk-Datei auf der Karte abzulegen, was sich natürlich auch manuell erledigen lässt. Erweist sich ein Update im Nachhinein als nachteilig, kann man so mit Leichtigkeit auf eine vorige Version zurückgreifen. Gleiches gilt nach einem Factory-Reset: Auch wenn die Lieblings-App aus dem Playstore verschwunden sein sollte, das Monsterchen hat eine Kopie aufgehoben.



AppMonster

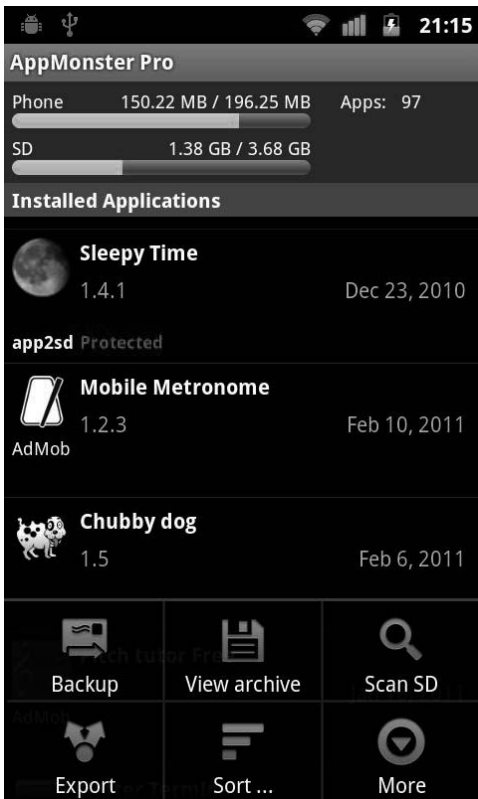


Bild 1.9: AppMonster Pro sichert die .apk-Dateien bei jeder Installation und bei jedem Update

Da kann man es fast als „nette Dreingabe“ betrachten, dass so einige Zusatzinformationen in der Appliste angezeigt werden: Etwa ob eine App mit Werbemodul (AdMob) daherkommt – was dann auch die Berechtigung für den Internet-Zugriff erklären könnte. Oder ob App2SD unterstützt wird. Des Weiteren hat man auch direkt Zugriff auf die Playstore-Seite der jeweiligen App – oder kann sie über Facebook, Twitter oder auch per Mail weiterempfehlen. Oder ganz anders herum: Sie schnell deinstallieren ...

Fairerweise sei hier noch auf die Einschränkungen der kostenlosen Version hingewiesen: Keine automatische Sicherung der Neuinstallationen, kein Batch-Restore, und auch die erweiterten Informationen (wie App2SD) werden hier nicht angezeigt. Backups lassen sich aber manuell erstellen und auch wiederherstellen. Aus eigener Erfahrung kann ich den Kauf der Vollversion wärmstens empfehlen!



OnTheFly Backup

Was *Titanium Backup* im Komplett-Bereich, ist *AppMonster* hier: Mir ist keine App bekannt, die dem Monsterchen das Wasser reichen könnte. Alles andere kommt allenfalls „recht nah heran“ – wie etwa das in Bild 1.10 gezeigte *OnTheFly Backup*, das jedoch seit 2010 nicht mehr aktualisiert wurde. Es ist annähernd mit der Gratis-Version vom

AppMonster vergleichbar: Alle Apps lassen sich manuell sichern, auch in mehreren Versionen. Zusätzlich unterstützt *OnTheFly Backup* allerdings das Batch-Restore – ein Feature, das bei *AppMonster* der Pro-Version vorbehalten ist.



Bild 1.10: *OnTheFly Backup* erlaubt das manuelle Sichern von .apk-Dateien

Keine der anderen mir bekannten Apps in diesem Sektor unterstützt – wie die beiden genannten Kandidaten – das simultane Speichern mehrerer Versionen (sodass man bei Bedarf zu einer älteren Version zurückkehren kann). Dies halte ich jedoch hier für essenziell: Für alles andere habe ich ja – dank *Titanium Backup* – mein Vollbackup. Anwender ohne *root* sehen das vielleicht ein wenig anders.

Ein spezieller Backup-und-Restore-Wunsch tritt meist dann ein, wenn das Amazon-Päckchen mit dem lang ersehnten neuen Androiden eingetroffen ist. Dann wird ausgepackt, herumgespielt, gerootet, die Konfiguration durchgeschaut, das Eine oder Andere ausprobiert ... Alles selbstverständlich, während der „Alte“ noch in Benutzung ist.

Und dann ist es soweit: „Da war doch noch was ...“ Genau: Wie kommen jetzt die Apps von A nach B? Klar, mit *Titanium Backup*. Also auf dem „Alten“ alles sichern, von der Karte auf





den Rechner kopieren, vom Rechner auf die Karte des „Neuen“ ... Besonders umständlich wird es dann, wenn beide Geräte noch länger parallel laufen sollen.



AppSync

Aber warum schreibe ich das alles so dramatisch, wenn ich nicht mal wieder etwas anbieten möchte? Es muss also offensichtlich eine einfachere Lösung geben. Die trägt den Namen **AppSync** und ist in Bild 1.11 zu sehen. Wo man auch erkennt: Die gewünschte App kann ruhig bereits auf beiden Geräten vorhanden sein. **AppSync** muss das sogar. Und auf beiden Geräten mit dem selben Passwort konfiguriert, kann die Party beginnen: Kopiere von Lokal nach Remote. Oder umgekehrt. Neu nach Alt. Oder anders herum. Oder gar nicht (*Cancel*).

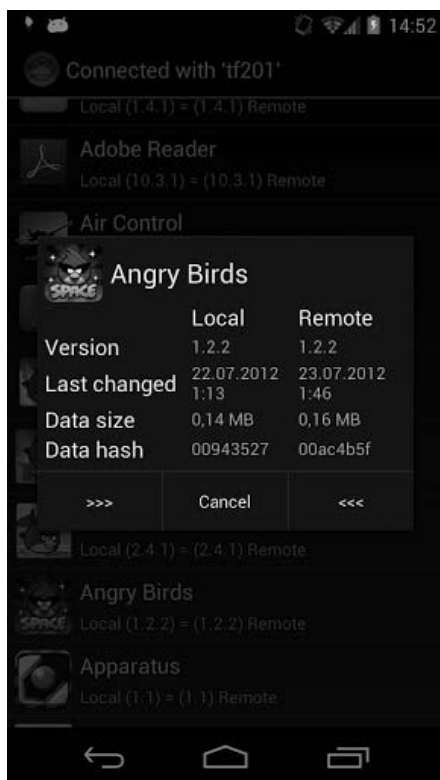


Bild 1.11: **AppSync** synchronisiert Apps und ihre Daten zwischen gerooteten Geräten

Und warum soll man sich dabei auf den „Umzug“ beschränken? Da drängen sich förmlich weitere Anwendungsgebiete auf: Unterwegs in der S-Bahn mit einer App auf dem Smartphone gewerkelt – und bei Ankunft zu Hause den aktuellen Stand auf's Tablet übertragen, wo es dann bequemer weitergehen kann. Oder morgens noch schnell den Spielstand vom Tablet auf das Smartphone schieben – damit man damit in der U-Bahn weiter daddelt, ohne dass der Spielstand leidet.



Ich bin mir sicher: Findige Geister wissen noch mehr Möglichkeiten. Und wen die Werbung stört, oder wer sich vor Begeisterung nicht mehr halten kann: Für ca. vier Euro gibt es im Playstore den passenden „Pro-Key“ zu erwerben ...

Kontakte, SMS & Co.

Für die Kontakte ist die Frage nach einem lokalen Backup schnell beantwortet: Es ist bereits dabei, auch wenn es gern übersehen wird. Einfach einmal die Kontakte-App starten, die Menü-Taste drücken und *Export* auswählen, schon landet die gesamte Kontaktliste mit allen Details, einschließlich Fotos, als VCard-Archiv auf der SD-Karte. Dieses Format versteht natürlich auch die Import-Funktion derselben App – ebenso aber nahezu jede Anwendung auf dem PC, die sich um Adressen kümmert.

Ebenfalls bereits im Auslieferungszustand an Bord: Die Synchronisation mit Google. Wer kein Problem damit hat, seine persönlichen Daten im Netz abzulegen, kann auf diese Weise Kontakte und Termine sichern. Google scheint das als selbstverständlich anzusehen, denn wenn man die zugehörigen Einträge in der Konfiguration nicht selbst findet und abschaltet, ist dies automatisch aktiv. Aber der Synchronisation ist ein eigener Abschnitt in diesem Kapitel gewidmet, daher soll hier die Erwähnung genügen.

Bei den eigenständigen Backup-Apps fange ich auch hier mit denen an, die möglichst Vieles abdecken. Und da käme **Pi.Soft Backup** (Bild 1.12) an erster Stelle: Die Vollversion kostet gut zwei Euro und verzichtet auf die allgegenwärtige Internet-Berechtigung, wie auch die ebenfalls im Playstore verfügbare Gratis-Testversion (nur in der Laufzeit auf 15 Tage beschränkt, sonst voller Funktionsumfang). Hier ist man sich offensichtlich der Sensibilität persönlicher Daten bewusst, was für mich und andere „Paranoiker“ eine erfreuliche Tatsache ist.



Pi.Soft Backup



Bild 1.12: *Pi.Soft Backup* sichert Anruflisten, Lesezeichen und Textnachrichten

Wie der abgebildete Screenshot erkennen lässt, kümmert sich die App um Anruflisten, Favoriten, SMS/MMS sowie Lesezeichen und den Browserverlauf. Die Kontakt-Sicherung haben wir bereits in der Kontakte-App integriert – somit würden hier nur noch die Kalenderdaten zu einem vollständigen PIM-Backup fehlen.



Mobile Backup II

Kalender, Kontakte, SMS und Anruflisten sichert **Mobile Backup II** auf die Karte (hier würden also Favoriten und Lesezeichen auf der Strecke bleiben). Bei den angeforderten Berechtigungen (u. a. Internet, Telefonnummern anrufen) würde ich diese App ohne passenden Schutz (beispielsweise durch LBE) aber lieber nicht installieren.



SMS Backup & Restore

Doch auch für Einzelaufgaben stehen Apps bereit. So kümmert sich beispielsweise **SMS Backup & Restore** (Bild 1.13) um – der Name sagt es schon – die Sicherung und Wiederherstellung der Kurznachrichten. Zwar unterstützt die App (noch) keine MMS – um SMS kümmert sie sich jedoch vorzüglich, wie auch zahlreiche Playstore-Kommentare und -Bewertungen (4,7 Sterne bei über 13.000 Bewertungen für die Gratis-Version, 4,9 Sterne bei ca. 50 Bewertungen für die werbefreie Donation-App zu knapp anderthalb Euro) belegen.

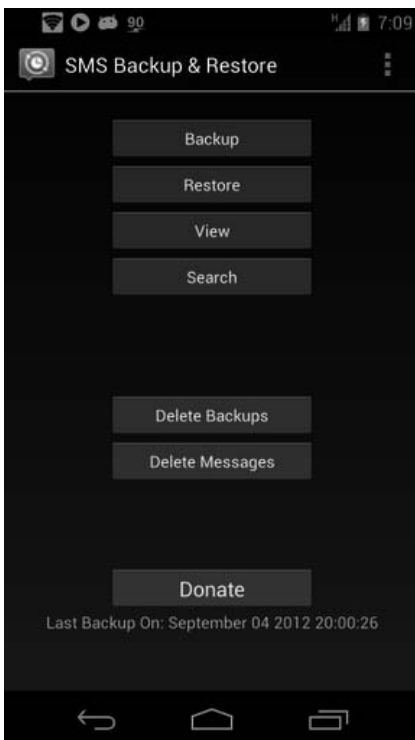


Bild 1.13: **SMS Backup & Restore** ist der Spezialist für Kurznachrichten

Erstellte Sicherungen lassen sich auch am Androiden sichten. Da für den Export das XML-Format gewählt wurde, steht auch einer Weiterverarbeitung am PC nichts im Wege. Vor der Erstellung eines Backups lässt sich auswählen, ob man alles oder nur ausgewählte Konversationen sichern möchte. Auch ein Versand per Mail (hier wird die erzeugte Backup-Datei an die gewählte Mail-App übergeben) ist möglich.

Die Internet-Berechtigung wird nur in der Gratis-Version (für Werbung) benötigt. Durch Zahlung eines Lösegelds in Höhe von knapp anderthalb Euro erhält man eine von Werbung befreite Vollversion, die diese Berechtigung auch nicht mehr anfordert.

Tipp am Rande: Einige Kommentare erwähnen explizit den mit dieser App erfolgreich vollzogenen „Umzug“ der Kurznachrichten zu einem neuen Telefon sowie die Wiederherstellung nach einer Neuinstallation ...

Wer zusätzlich noch MMS-Unterstützung benötigt, kann u. a. für knapp drei Euro auf **Txtract MS & SMS Backup** zurückgreifen. Hier erhält man ein gut sortiertes Archiv (XML/HTML), das sich u. a. prima am PC einsehen lässt – also eine gute Sache für die (permanente) „Langzeit-Archivierung“.



Txtract MS & SMS
Backup

Für die Anrufprotokolle käme **Call Logs Backup & Restore** in Frage. Der Name klingt so nach ...? Ja, genau: Es handelt sich um den gleichen Entwickler wie beim gerade genannten **SMS Backup & Restore**. Und auch hier wieder Topp-Bewertungen (4,7 Sterne). Sieht von den Screenshots her auch wieder genauso aus – und ersetzt man „SMS“ durch „Anrufprotokoll“, gleichen sich auch die Features weitgehend. Größter Unterschied: Hier gibt es keine Bezahlversion, mit der man die „Internet-Berechtigung“ loswerden könnte. Was übrigens auch für das aus dem gleichen Hause stammende **APN Backup & Restore** gilt, welches sich um die APNs (Zugangspunkte zum Internet) kümmert ...

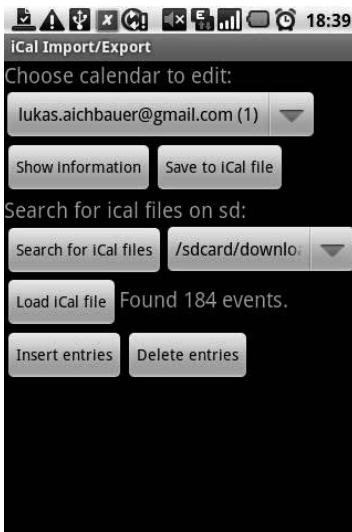


Call Logs Backup
& Restore

Womit wir bei den Kalendern angekommen wären, die ja – im Gegensatz zum Adressbuch – von Haus aus keine Export-Funktion (außer dem Google-Sync) haben. Hier schafft die App **iCal Import/Export** (Bild 1.14) Abhilfe, indem sie ihn im iCal-Format exportiert. Natürlich ist auch ein Import aus diesem Format möglich, sogar über das Web: So lassen sich beliebige andere Kalenderdaten (z. B. Feiertage) importieren. Empfehlung: Sollte das jemand für Feiertage nutzen wollen, besser einen separaten Kalender dafür anlegen – dann wird man ihn später leichter wieder los ... Alternativen für ein lokales Kalender-Backup sind mir leider nicht bekannt.



APN Backup &
Restore



iCal Import/Export

Bild 1.14: *iCal Import/Export* sichert die Kalender-Einträge im iCal Format – und kann sie auch wieder aus selbigem Einlesen

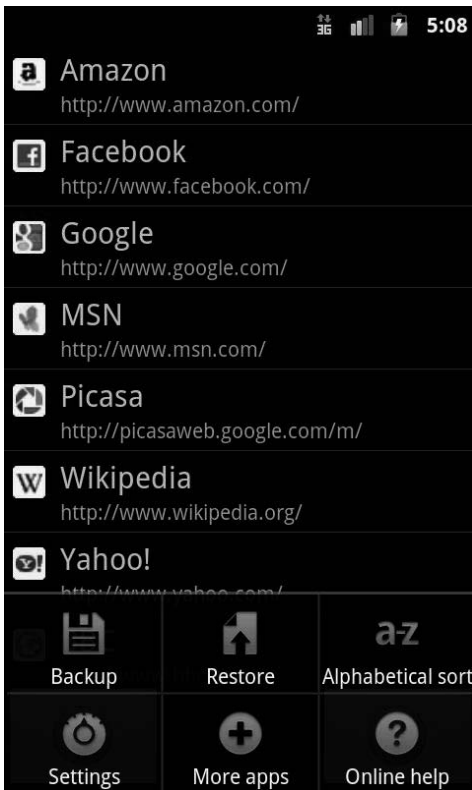
Die integrierte Lösung für die Kontakte habe ich bereits im ersten Satz genannt (die alternativen Apps können da auch nicht mehr). Wenden wir uns also zu guter Letzt noch den Lesezeichen zu. Für eine einfache Sicherung und Wiederherstellung steht hier **Backup Bookmarks** zur Verfügung, das die Daten im XML-Format speichert. Da es sich dabei um ein textbasiertes Datenformat handelt, lässt sich das Backup auch mit einem Blick in die Datei überprüfen – und sollte die Wiederherstellung einmal fehlschlagen, sind die Daten damit noch lange nicht futsch: Datei im Browser öffnen, jeden Link einzeln anklicken und erneut als Lesezeichen hinzufügen funktioniert sodann als Notlösung ...



Backup Bookmarks

Oder man greift zu **Bookmark Sort & Backup** (Bild 1.15) und holt sich damit gleich eine Sortierfunktion hinzu. Letztere lässt sich im „Automatik-Modus“ betreiben, um alle Lesezeichen alphabetisch zu sortieren – oder auch manuell, wobei man Lesezeichen einzeln in ihrer Position verschieben kann.

Für die Sicherung (und Wiederherstellung) von Lesezeichen verwendet diese App interessanterweise das HTML-Format, welches auch bei Firefox (oder dem Internet-Explorer) zum Einsatz kommt. Hübscher Nebeneffekt: Wer noch gar keine Lesezeichen angelegt hat, kann auf diese Weise die aus dem PC-Browser übernehmen.



Bookmark Sort &
Backup

Bild 1.15: *Bookmark Sort & Backup* eignet sich nicht nur zum Sichern, sondern auch zum Sortieren der Lesezeichen

Die Anwender sind, soweit man das den Playstore-Kommentaren entnehmen kann, durchweg zufrieden bis begeistert. Auch wenn hie und da berichtet wird, dass die Sortierfunktion mit Gingerbread (Android 2.3.x) ihre Probleme hat: Backup und Restore funktionieren einwandfrei! Warum die App allerdings „nach dem Booten starten“ möchte, ist nicht so ganz nachvollziehbar. Die Internet-Berechtigung dient dem Werbebezug und kann gegen einen knappen Euro mit der Vollversion „beseitigt“ werden.

Backup in die Cloud

Das ist ja der letzte Schrei und furchtbar modern: Alles ab in die Wolke. Schon Reinhard Mey wusste (und weiß): „Über den Wolken muss die Freiheit wohl grenzenlos sein ...“ Da können wir unsere Backups ja gleich einmal hinterher schieben (um uns später zu wundern, wo sie teilweise wieder herabregnen).

Bordmittel

Für die Wolke gibt es sie tatsächlich – jedoch sind sie extrem eingeschränkt und oftmals auch recht unzuverlässig. So finden sich in der Gerätekonfiguration unter *Datenschutz* die Optionen *Meine Einstellungen sichern* sowie *Autom. Wiederherstellung*, die sich beide auf das *Google Backup* beziehen. Details dazu sind in diesem Buch bei der entsprechenden Einstellung ausgeführt. Hier nur so viel: Es werden nur einige Apps und ihre Einstellungen unterstützt sowie einige Android-Einstellungen (etwa Lesezeichen und WLAN-Netzwerke). Daher an dieser Stelle lediglich die „Erwähnung der Vollständigkeit halber“.

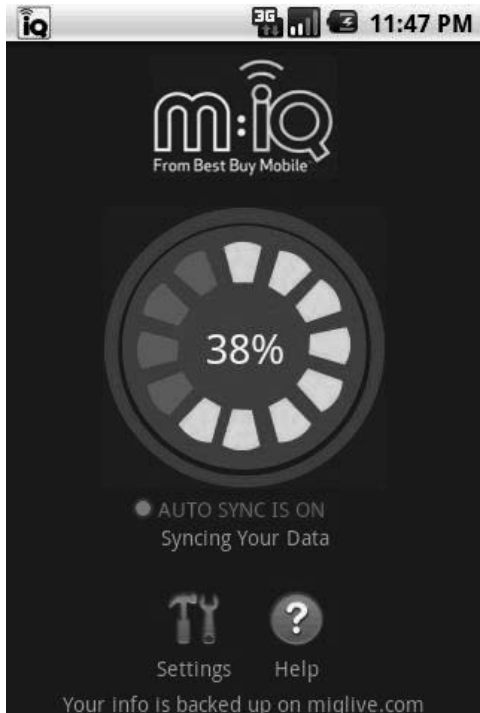
Komplettsicherungen



DroiDrive

Sprite Backup wurde ja bereits bei den lokalen Komplettsicherungen genannt, kann aber auch in die Cloud sichern. Auf eine ganz andere Weise erledigt dies *DroiDrive*, indem es das ganze Dateisystem auf den Server des Anbieters kopiert. Jedenfalls soweit man auf selbiges Zugriff hat.

Um so ziemlich alles (außer Apps und ihren Einstellungen) kümmert sich *mIQ* (Bild 1.16): Kontakte, Texte, Kalendereinträge, Anruflisten, Fotos, Videos und Voicemails schiebt es auf den/die Server des Anbieters. So ganz nebenbei möchte es dabei



mIQ

Bild 1.16: *mIQ* bietet ein recht umfassendes Backup in die Cloud

auch „nach dem Booten starten“ (automatische Synchronisation, siehe Screenshot) sowie SMS empfangen und auch senden (Huch? Wozu das?). Ähnliches leistet auch **Pleex Mobile Backup** – mit Ausnahme des „nach dem Booten Startens“ sowie der damit verbundenen automatischen Synchronisierung (aber inklusive des SMS-Verschickens).



Pleex Mobile
Backup

Da gibt es noch eine ganze Reihe weiterer Kandidaten, die diese Aufgabe mehr oder weniger vollständig erfüllen wollen – zu finden in der bereits bei den lokalen Backups genannten Übersicht. So richtig überzeugen konnte mich keine dieser Lösungen – was aber nicht zuletzt auch an meiner diesbezüglich etwas konservativen Einstellung liegen mag.

Kontakte, SMS & Co.

Kontakte und Kalender? Na, diese Frage beantwortet sich bei Android eigentlich fast von selbst: Wenn man dem nicht explizit einen Riegel vorschiebt, landen diese Daten automatisch auf den Google-Servern – und werden bei bestehender Datenverbindung permanent synchron gehalten (außer, wenn der entsprechende Google-Dienst mal wieder verrückt spielt). Vergleichbare Alternativen, abgesehen von den obigen, sind mir nur mit Providerbindung in Übersee bekannt. Sofern man sich nicht selbst etwas gebaut hat – doch dazu später mehr.

Für SMS und MMS gibt es jedoch mit **SMS Backup** + einen Kandidaten, der durchaus einen näheren Blick wert sein könnte: Von über 11.000 Anwendern mit durchschnittlich 4,6 Sternen bewertet, das will schon etwas heißen! Neben den genannten Kurz- und Multimedia-Nachrichten kümmert sich die App auch noch um die Anruflisten und speichert alles (bei Nutzung unterschiedlicher Labels) im eigenen Google-Mail-Account bzw. -Kalender. Eine Wiederherstellung ist, mit Ausnahme von MMS, ebenfalls möglich. Übrigens möchte auch diese App nach dem Booten starten – mit einer automatischen Synchronisation dürfte also zu rechnen sein.



SMS Backup +

Nebeneffekt: Wenn SMS, MMS und Anruflisten automatisch im Google-Mail-Account bzw. -Kalender landen, kann man sie natürlich auch von jedem beliebigen PC ohne Zugriff auf das Telefon lesen. Also Vorsicht, wem man die Zugangsdaten gibt – denn diese Person sieht dann sehr wohl, wann man mit wem telefoniert hat ...

Wer keine MMS zu verwalten hat und die Anrufliste ignorieren kann, der mag vielleicht alternativ zu **Gschickt** greifen. Neben der Online-Sicherung kommen bei dieser App einige Zusatz-Funktionen dazu, wie etwa die Nutzung von (oft kostengünstigeren) Online-SMS-Services (genannt sind hier „sms-kaufen“ und „innosend“), Statistiken über den SMS-Ver-sand, ein SMS-Editor mit Smileys, Zeichenspar-Funktion, Sprechblasen sowie anpassbarer Schriftgröße, Empfangsberichte, Text-to-Speech (TTS) und Nachrichten-Threads.



Bild 1.17: *SMS Backup +* sichert Kurznachrichten und Anruflisten in den eigenen Google Mail Account

Die erweiterte Vollversion schlägt mit knapp zwei Euro zu Buche. Sie bietet unter anderem Unterstützung für „lange“ SMS mit bis zu 800 Zeichen, Textbausteine sowie mehrere Identitäten (Absender-Nummern).



Gschickt

Für die zusätzlichen Web-SMS-Dienste sind natürlich separate Accounts notwendig. Gleiches gilt in Bezug auf die Online-Sicherung für die Website von *Gschickt* selbst. Dass die App die Berechtigung zum Versenden von Kurznachrichten fordert, sieht sicherlich jeder ein. Auch der Zugriff auf das Adressbuch ist nachvollziehbar (wenn auch etwas kritisch im Zusammenhang mit der ebenfalls erklärbaren Berechtigung zum Internet-Zugriff). Nachdenklich stimmt hingegen,

dass sie zusätzlich Telefonnummern anrufen möchte. Aus der Beschreibung ist dafür kein Grund zu erkennen, eine Erklärung dazu sucht man in der App-Beschreibung ebenfalls vergeblich; auch auf der Website wurde ich diesbezüglich nicht fündig.

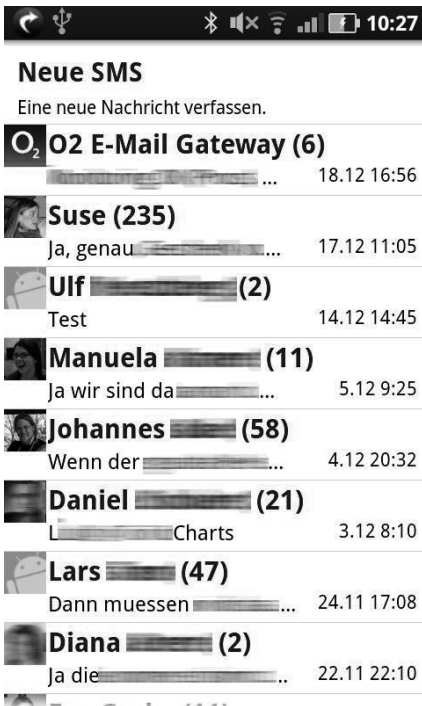


Bild 1.18: *Gschickt* sichert SMS-Nachrichten, bietet aber auch kostengünstige Versandmöglichkeiten

Synchronisation

Die Grenzen zwischen einem Online-Backup und der Synchronisation sind fließend. Kalender und Kontakte werden unter Android beispielsweise automatisch mit den entsprechenden Google-Accounts synchronisiert – manch einer sieht das als Backup an. Im Prinzip kann man sagen: Die Synchronisation ist eine Form des Backups – ein Backup aber nicht zwangsweise eine Synchronisation. Darüber hinaus gibt es Synchronisation und Synchronisation: Man kann, wie soeben anhand der Google-Dienste aufgezeigt, die Daten „mit der Cloud“ synchronisieren oder aber mit einem eigenen Rechner.

Beim Synchronisieren arbeitet man in der Regel mit zwei „gleichwertigen Kopien“ (im Unterschied zum Backup, bei dem die Daten meist komprimiert abgelegt werden). Die Daten liegen also auf der „Gegenseite“ genau so vor, wie sie es lokal tun. Und oftmals arbeitet man mit den Daten auch auf beiden Seiten: fügt etwa Termine sowohl auf dem Androiden, als auch vom PC aus auf dem Google-Server hinzu.

Unterscheiden kann man unter anderem nach der Gegenseite der Synchronisation: Landen die Daten auf „fremden Servern“ (also wieder in der Cloud) oder auf einem eigenen Rechner? Ein nicht unwesentliches Kriterium, das ich im Folgenden auch besonders berücksichtigen werde – nicht jeder gibt schließlich seine Daten freiwillig heraus.

Kontakte und die Cloud



XING Sync

Zuallererst wären da die beliebten sozialen Netzwerke, die sich in die Kontaktliste integrieren lassen. Beste App in diesem Bereich: **XING Sync** (Bild 1.19). App ist da eigentlich das grundverkehrte Wort, denn die sucht man nach der Installation vergeblich. „Synchronisations-Adapter“ trifft es eigentlich eher oder auch „Content Provider“. Wie am Screenshot zu erkennen, klinkt sich **XING Sync** nämlich in das Menü unter „Konten & Einstellungen“ ein und sorgt dort für einen zusätzlichen Eintrag – allerdings erst, wenn man dies nach Betätigen des „Hinzufügen“-Buttons veranlasst hat. Hier werden die XING-Zugangsdaten hinterlegt, die Synchronisation aktiviert – und kurz danach tauchen die XING-Kontakte im Adressbuch auf. Wird einem die Liste hier zu lang, und möchte man das Ganze wieder loswerden: Keine Panik, die Daten sind nicht bunt mit den Standard-Kontakten gemischt worden. Einfach an der genannten Stelle das Konto wieder entfernen, und weg sind sie. Bitte beachten: **XING Sync** funktioniert nur für XING-Premium-Accounts und kostet übrigens einen Euro.

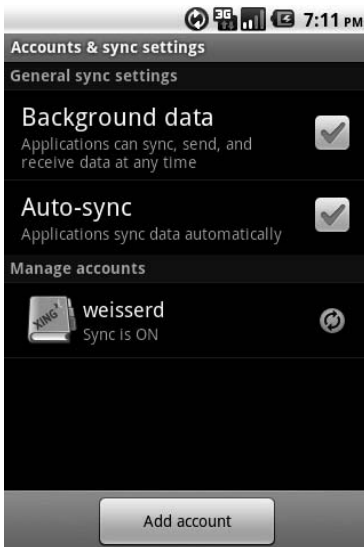


Bild 1.19: **XING Sync** bindet Kontakte aus dem Netzwerk XING ein



XING-App

Auch die originale **XING-App** soll die Synchronisation mittlerweile beherrschen. Ob sie das genauso gut hinbekommt, ist mir nicht bekannt – dafür ist sie jedoch gratis und fast gleich gut bewertet.

Von XING zu den Mitbewerbern: Orkut-Kontakte lassen sich mit **Orkut Contact Sync** in das Adressbuch einbinden. Wer hier vergeblich nach der Installation die App sucht, fühlt sich eventuell an die Beschreibung von **XING Sync** erinnert. Und verfährt hier erfolgreich analog zu selbiger.

Ich höre schon die Frage: Warum wird hier nichts von Facebook erwähnt? Da scheint es einfach nichts Vernünftiges zu geben. Was sicher nicht daran liegt, dass ich kein großer Fan von Facebook & Co. bin: Die beste Bewertung liegt hier bei 3,5 Sternen, für die entweder keinerlei Details zu sehen sind – oder die App funktioniert einfach nicht mehr mit aktuellen Android-Versionen. Tut mir leid für die danach Suchenden – aber es besteht ja immer noch die Hoffnung, dass mir da etwas entgangen ist.



Orkut Contact
Sync

Kontakte, Kalender und mehr mit eigener Hardware synchronisieren

Für die Kalender-Synchronisation hat sich in diesem Bereich eine noch recht junge App schnell an die Spitze gesetzt: **ICSSync** (Bild 1.20) kann mehrere *.ics-Dateien mit lokalen Kalendern synchron halten. Dafür wird für jede Quelle ein eigener lokaler Kalender angelegt. Die Quellen können dabei auf einem FTP- oder auch einem CalDav-Server liegen. Ein einseitiger Import (etwa von Feiertagen) ist ebenso möglich wie eine bidirektionale Aktualisierung, bei der die Kalenderdatei gleichzeitig von mehreren Clients zum Lesen und Schreiben genutzt wird. Der Abgleich kann sowohl manuell als auch automatisiert erfolgen – das wäre also so etwas wie Google-Kalender ohne Google, wenn man das Web-Interface einmal vernachlässigt.



ICSSync

The screenshot shows the ICSSync app interface on an Android device. At the top, there's a status bar with icons for signal, battery, and time (12:28). The app has a dark theme. The main form includes:

- Feed URL (e.g. 'https://my.host.com/ical.ics')**: A text input field containing "https://my.host.com/ical.ics".
- Username (optional)**: A text input field containing "coolUserName23".
- Password (optional)**: A text input field with masked characters ".....".
- Local calendar name (creates a new one)**: A text input field containing "Vacation".
- Read only (don't write to remote)**: A checked checkbox.
- Allow untrusted certificates**: A checked checkbox.
- Pick color**: A button.
- Set sync interval**: A dropdown menu currently showing "use global sync-interval".

Bild 1.20: **ICSSync** hält lokale Kalender mit .ics-Dateien (beispielsweise auf CalDav-Servern) synchron

Ist eine automatische Synchronisierung gewünscht, lässt sich bei *ICSSync* das Intervall für jede Quelle individuell festlegen. Eine Synchronisation abhängig vom verfügbaren Netzwerk (etwa nur bei bestehender WLAN-Verbindung) ist ebenfalls möglich.

Die Testversion ist für 20 Tage in vollem Umfang einsatzfähig. Will man sie weiterhin nutzen, muss man für knapp anderthalb Euro einen Freischaltcode erwerben – was sowohl im Google Playstore (Zahlung per Kreditkarte) als auch bei AndroidPIT (Zahlung per Kreditkarte oder Paypal) möglich ist.



Funambol Sync

Eine ganze Menge mehr „Services“ lassen sich mit **Funambol Sync** abgleichen, wie der Screenshot zeigt: Kontakte, Kalender, Bilder, Videos und sonstige Dateien. Am liebsten sieht es der Anbieter natürlich, wenn auf der „anderen Seite“ seine eigenen Server werkeln – man dazu also die Services von *Funambol.com* selbst nutzt. Das ist selbstverständlich eine Möglichkeit, aber nicht die einzige. Auf *Funambol.org* stehen sowohl Server-Software für Linux und Windows (beides für 32Bit und 64Bit), als auch PC-Clients für Windows und Mac OS bereit.



Bild 1.21: *Funambol* bietet umfangreiche Synchronisations-Möglichkeiten

Ganz unabhängig davon, gibt es auf der letztgenannten Website auch Lösungen für zahlreiche PC-Programme wie Mozilla Thunderbird und Gnome Evolution und viele weitere.



<http://www.androidpit.de/de/android/forum/thread/412829/>

So gesehen deckt *Funambol* wohl die breiteste Palette ab. Wer mehr dazu erfahren möchte, sollte also dort einmal vorbeischaun – und findet dann unter anderem auch einige Video-Demos und -Tutorials, Online-Hilfe und Kontakt zur zugehörigen Community.

Weitere Apps zu den letzten beiden Themen finden sich übrigens in der **Übersicht** im AndroidPIT-Forum.

Dateien und Verzeichnisse in der Cloud

Unbewusst hat Reinhard Mey die Cloud bereits 1971 in seinem Lied „Über den Wolken“ besungen. Hier einmal eine zeitgenössische Interpretation des Refrains:

Über den Wolken [total abgehoben und völlig überbewertet]

Muss die Freiheit wohl grenzenlos sein. [die Daten werden über die halbe Welt verstreut!]

Aller Kummer, alle Sorgen, sagt man, [genau weiß es keiner]

Blieben darunter verborgen, und dann, [und niemand schaut da wirklich durch]

Würde, was uns groß und wichtig erscheint [Megabytes, Gigabytes]

Plötzlich nichtig und klein. [angesichts der verfügbaren Tera- und Petabytes]

Bei dem Wort „Cloud“ denkt der Android-Jünger wahrscheinlich zuerst an Google, dann an die Dropbox. Danach folgt wahrscheinlich erst einmal eine ganze Weile gar nichts. Dennoch möchte ich hier weder mit Google noch mit Dropbox beginnen – sondern eine überaus interessante Alternative zu letzterer vorstellen:

Der Dienst nennt sich **Wuala**, und dahinter steht u. a. der bekannte französische Festplatten-Hersteller LaCie. Die Server finden sich in Frankreich, der Schweiz und Deutschland – sind also gar nicht so weit weg.

Aber das sind alles nur „politische Details“. Interessanter sind einige der technischen „Kleinigkeiten“: Etwa, dass dieser Cloud-Service sowohl für Android als auch unter Linux, Mac OS und Windows Clients bereitstellt. Oder dass die Daten in der Cloud verschlüsselt abgelegt werden – wobei die Verschlüsselung auf dem Client erfolgt. Ferner lassen sich die Daten für andere freigeben, sogar Gruppen kann man anlegen: So steht dem Teamwork eigentlich nichts im Weg. Als Sahnehäubchen wurde dem Ganzen eine Versionierung spendiert: Die ältere (oder gelöschte) Version einer Datei zu „restaurieren“ stellt hier also kein großes Problem dar.

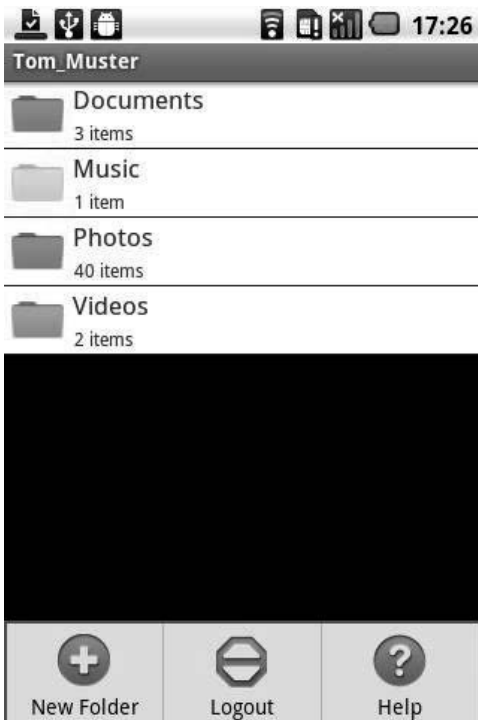


Bild 1.22: Wuala speichert die Daten von vornherein verschlüsselt und bietet Clients für Android, Linux, Mac OS sowie Windows

Der „offizielle Android-Client“ (Bild 1.22) trägt den Namen des Dienstes: **Wuala**. Er unterstützt diese Funktionalitäten natürlich. Ein Drittanbieter steuert noch weitere Apps bei: etwa eine Galerie, einen Music Player und einen alternativen Sync-Client, der allerdings nur lesend auf die Wuala-Cloud zugreifen kann.

Eine der größten und bekanntesten „Wolken“ ist sicher **Dropbox** – mit Client-Software für Linux, Mac OS und Windows auf dem heimischen Rechner sowie Android, Blackberry, iPad und iPhone auf den mobilen Geräten wird hier sicher auch die größte Bandbreite von Geräten unterstützt. Darüber hinaus gibt es für Entwickler die Möglichkeit, durch die Verwendung der bereitgestellten API die **Dropbox** direkt in ihre Applikation einzubinden – was bei vielen Apps auch bereits passiert ist. Um welche Apps es sich dabei handeln könnte, kann man im Dropbox-App-Verzeichnis (<http://www.dropbox.com/apps>) für alle beteiligten Plattformen (auch separat gefiltert) nachschlagen, wobei diese Liste keinesfalls vollständig ist.



Dropbox

Aber schauen wir uns doch ausgewählte Clients einmal kurz an. Da wäre natürlich zuerst die offizielle **Dropbox-App** (siehe Bild 1.23), die genau wie der Dienst einfach nur **Dropbox** heißt. Sie kümmert sich in erster Linie um die Synchronisation von Dateien und Verzeichnissen, wozu sie einen „Spiegel“ der im Service bereitgestellten „Online-Fest-

platte“ auf dem Gerät bereithält. Wird dort eine Datei abgelegt oder verändert, bemerkt der Service das, und veranlasst eine Online-Aktualisierung – gegebenenfalls wartet sie damit auch, bis eine Netzverbindung besteht. Umgekehrt erfolgen auch Aktualisierungen aus der Cloud, falls eine Datei von einem anderen Client modifiziert wurde. So sind alle Beteiligten stets auf dem aktuellen Stand.

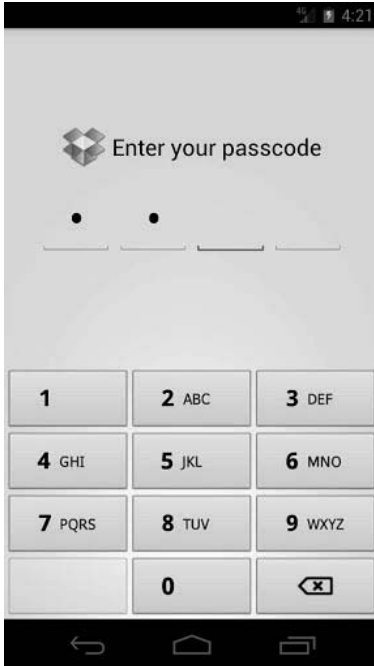


Bild 1.23: *Dropbox* ist der bekannteste Cloud-Service. Abgebildet ist hier der offizielle Client

Ebenso lassen sich Dropbox-Ordner für Freunde und Verwandte freigeben, E-Mail-Anhänge direkt in der Dropbox abspeichern oder Dokumente direkt in der Dropbox bearbeiten ... 4,7 Sterne bei weit über 70.000 Bewertungen zeugen nicht nur von reger Nutzung, sondern auch von vielen zufriedenen Anwendern.

Für die Automatisierung mit *Tasker* (vgl. Abschnitt 2.5) stehen gleich zwei Plugins zur Verfügung: ***Dropbox Sync for Tasker Locale*** (Bild 1.24) greift direkt auf die offizielle Dropbox-API zu und benötigt so keine zusätzliche App. Der Name verrät bereits, dass sich dieses Plugin auch mit *Locale* verwenden lässt – das volle Potenzial wird aber nur mit *Tasker* ausgeschöpft, indem sich z. B. auch Variablen in Datei- und Verzeichnisnamen verwenden lassen.



Dropbox Sync for
Tasker Locale



Bild 1.24: *Dropbox Sync for Tasker Locale* bindet die Synchronisation in die beliebten Automatisierungs-Apps **Tasker** und **Locale** ein



DropSpace Plugin
for Tasker



DropSpace



DropSnap

Das **DropSpace Plugin for Tasker** greift hingegen auf die App **DropSpace** zurück, mit der sich Dateien und Verzeichnisse für die Synchronisation mit der Dropbox auswählen lassen. Diese werden in einer Liste zusammengefasst und entweder „on Demand“ per Widget oder „automatisch zeitgesteuert“ per Service synchronisiert.

Ein weiterer Dropbox-Client wäre in diesem Zusammenhang **DropSnap**. Auch hier lassen sich wieder Verzeichnisse zur Synchronisation konfigurieren. Ferner gibt es einige Möglichkeiten, die Synchronisation an die eigenen Bedürfnisse anzupassen: Nur bei vorhandener WLAN-Verbindung synchronisieren? Soll überhaupt automatisch synchronisiert werden? Fotos gleich nach dem „Schießen“ automatisch hochladen? Das Synchronisationsintervall lässt sich bei dieser App ebenfalls einstellen.

In Sachen Verschlüsselung sah es bislang ein wenig mau aus, wollte man dabei zu verschiedenen Systemen kompatibel sein (also etwa vom Androiden *und* vom PC unter Windows *und* Linux auf die Daten zugreifen). Besserung zeichnet sich bereits ab: **BoxCryptor** gibt es jetzt auch für Android. Die App eignet sich für Dropbox und Google

Drive und legt die Daten mit AES-256 verschlüsselt auf dem jeweiligen Server ab. Die Verschlüsselung erfolgt dabei, wie auch bei zuvor erwähntem *Wuala*, auf dem Gerät des Anwenders.



BoxCryptor

Einen weiteren Kandidaten möchte ich an dieser Stelle noch nennen: **DCD CloudSync** (Bild 1.25; man beachte den Tornado zwischen den oberen beiden Buttons, der hoffentlich nicht in Bezug auf die Daten bedeutet: „Up, up – and away...“). Ganz frisch auf dem Markt, kümmert diese App sich um Dateien und Verzeichnisse in der Cloud von Google. Wer einen Google-Account hat (also nahezu jeder Android-Nutzer), kann sich hier Speicher freischalten lassen. Voraussetzung ist allerdings, dass eine Kreditkarte mit dem Account verknüpft ist – auch wenn der Service selbst gegenwärtig kostenlos sein soll. In der Gratis-Version kann man mit **DCD CloudSync** genau einen Ordner verwalten; die Pro-Version für knapp drei Euro enthält dieses Limit nicht. Eine Synchronisation kann automatisch bei jeder Änderung, in vorgegebenen Zeitintervallen oder auch manuell erfolgen.



DCD CloudSync

Bild 1.25: **DCD CloudSync** kümmert sich um die Daten in der Google Cloud

Eine Übersicht zur Cloud findet sich wieder im **Forum** bei AndroidPIT.



<http://www.androidpit.de/de/android/forum/thread/433708/>

Dateien und Verzeichnisse auf eigener Hardware

Zugegeben: Nicht jeder kann sich gleich einen fetten Serverpark in den Keller stellen. Aber hey, auch Microsoft hat einmal ganz klein in einer Garage angefangen. Und wenn wir gerade vom Windows-Hersteller sprechen: Den kann man doch auch freigeben. Ich meine den Speicherplatz auf dem Windows-Rechner. Auf Linux- und Mac-OS-Rechnern heißt es dazu: „Tanze Samba mit mir ...“, denn hier gibt es den freien Samba-Server – bei den meisten Linuxen von Haus aus im Repository enthalten und auch für Mac OS zu haben. Auch NAS-Systeme bieten dies an, verbrauchen im Vergleich zum herkömmlichen PC kaum Strom und sind mittlerweile auch recht erschwinglich. So lässt sich Speicherplatz im heimischen Netzwerk zur Verfügung stellen – und darauf können dann auch unsere Androiden zugreifen.



AndSMB

Beispielsweise mittels **AndSMB** (Bild 1.26), einem SMB-Client für Android. Diese App erlaubt Zugriffe auf Windows-Freigaben ebenso wie auf Samba-Freigaben eines Linux- oder Mac-OS-Rechners, handelt es sich doch um das gleiche Übertragungs-Protokoll. Ein Dateibrowser ist in der App enthalten und erlaubt sowohl den Up- als auch den Download. Automatisiert man das Ganze nun, was mit dieser App möglich ist, hat man eine Synchronisation von Ordnern – und somit eine eigene minimale Cloud.

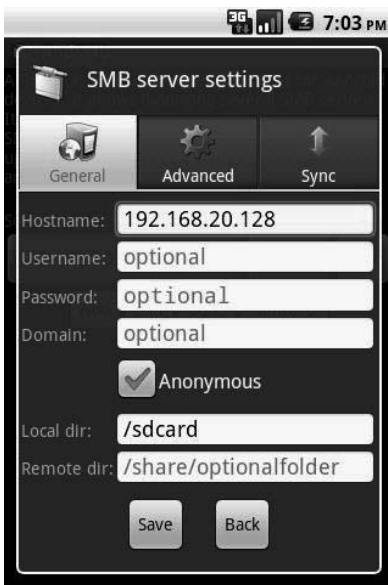


Bild 1.26: **AndSMB** erlaubt den Zugriff auf Samba- und Windows-Freigaben

Alternativ könnte **Sweet Home** (Bild 1.27) zum Einsatz kommen. Die Beschreibung der Pro-Version dieser App bringt es auf den Punkt: Keine Kabelsuche, auch muss man den

Androiden nicht mehr umständlich zerlegen, um die SD-Karte zu entnehmen: Sobald man zu Hause ankommt und sich der Androide ins heimische WLAN verbindet, werden die Daten automatisch synchronisiert. Die Gratis-Version punktet (laut Beschreibung) mit häufigen Updates (sowie dem unvermeidlichen „Nagging“), während die Bezahlversion gut getestet und stabil ist. Benutzer der freien Version sind also Beta-Tester ...

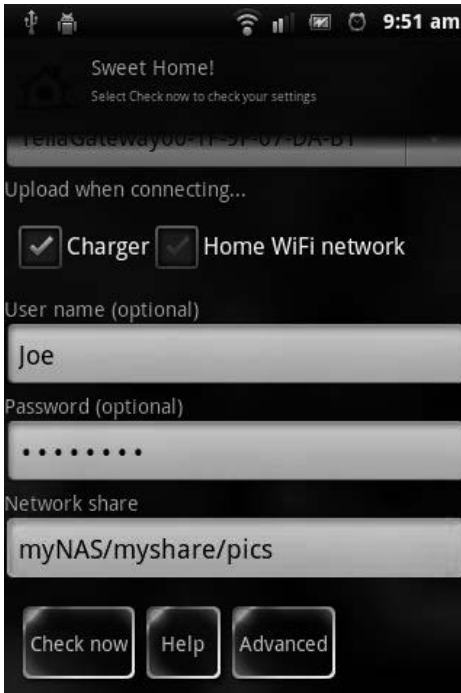
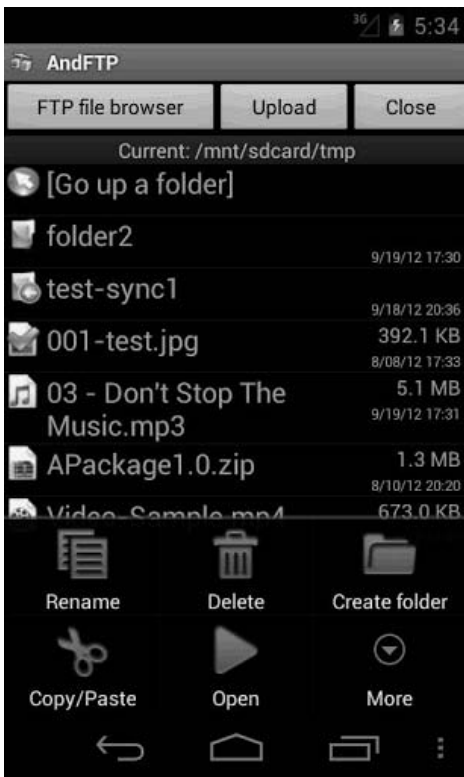


Bild 1.27: Sweet Home – Automatische Synchronisierung bei Ankunft im heimischen WLAN

Da Samba- bzw. Windows-Freigaben in der Regel jedoch auf das jeweilige lokale Netzwerk beschränkt sind, ist man mit einer derartigen Mini-Wolke örtlich recht limitiert. Für viele Fälle mag dies ausreichend sein – und was nicht über fremde Netze geht, ist auch vor „Schnüfflern in der Mitte“ sicherer. Wird jedoch ein Zugriff auch von unterwegs gewünscht, greift man am Besten zu einem der folgenden Multi-Talente, die sich auch auf Protokolle wie FTP[S] und SFTP/SSH verstehen. Und auf der Gegenseite natürlich zu einem passenden Server: SFTP/SSH sind unter Linux von Haus aus dabei, ein FTP-Server lässt sich auf allen Systemen relativ einfach aufsetzen – und verfügt man über einen eigenen Root-Server, z. B. für seine Webseiten, sollte einer der beiden Dienste (SSH-Server und/oder FTP-Server) ohnehin bereits vorhanden sein.

Eine passende App auf unserem Androiden wäre dann beispielsweise **AndFTP** (Bild 1.28). Topp bewertet, bringt sie gar einen Manager für die auf dem Server abgelegten Dateien mit. Sie versteht sich auf die Protokolle FTP, FTPS, SCP sowie SFTP und kann mehrere

Serverkonfigurationen verwalten. Neben Upload, Download und Synchronisation ist auch das Share-Menü sowie direkte Unterstützung für die Galerie eingebunden. Für SSH-Verbindungen (SCP) können überdies RSA/DSA-Schlüssel verwendet werden. SCP und Ordner-Synchronisation sind allerdings nur in der Pro-Version verfügbar.



AndFTP

Bild 1.28: *AndFTP* nutzt das FTP-Protokoll zur Synchronisation



FTPSyncX

Wer es jedoch besonders flexibel mag, auf einen „Remote Explorer“ verzichten kann und hauptsächlich Wert auf die Synchronisation legt, der sollte unbedingt einen Blick auf **FTPSyncX** (Bild 1.29) werfen: Wie beim gerade beschriebenen *AndFTP* werden auch hier die Protokolle FTP, FTPS sowie SFTP/SCP unterstützt, zusätzlich ist Samba mit an Bord. Die Testversion ist im Funktionsumfang völlig uneingeschränkt – sieht man vom Limit „zwei Server mit insgesamt vier Verzeichnissen“

einmal ab, was für einen Test (und oftmals auch für den Alltags-Einsatz) völlig ausreichend ist.

Okay – und was ist der Funktionsumfang? Synchronisieren, oder? Klar, aber wie? Und da stehen hier wirklich alle Türen offen: Einzelne Verzeichnisse oder gleich alle für einen Server definierten Verzeichnisse synchronisieren? Zeitgesteuert alle XX Minuten oder nur

manuell? Und wenn manuell: Aus der App heraus, über Widgets oder per Shortcut? Alles ohne großen Aufwand möglich. Die gewünschten Intervalle lassen sich auch für jedes Verzeichnis und jeden Server separat und unabhängig definieren.



Bild 1.29: Anders, als der Name es vermuten lässt, versteht sich **FTPSyncX** auf zahlreiche Protokolle

Naja, aber dann läuft die App also ständig im Hintergrund? Mir wäre es lieber, sie synchronisiert einmal, wenn ... Ein Fall für *Tasker* (siehe Abschnitt 2.5), eindeutig. Und auch für diesen ist ein Plugin bereits im Funktionsumfang enthalten – es sollte also kein Thema sein, die Synchronisation z. B. einmal automatisch anzustoßen, wenn man daheim ankommt und sich mit dem heimischen WLAN verbindet. Oder wenn man den Androiden in die Docking-Station steckt. Oder ...

Zumindest erwähnen sollte ich auch noch die App **FolderSync**, bei der an unterstützten Protokollen neben FTP, FTPS, und SFTP noch Web-DAV und Samba dazukommen. Und soll es doch einmal in die Wolke gehen, sind offensichtlich Dropbox und Amazons S3 ebenso mit von der Partie. Außerdem ist noch ein Datei-Manager integriert, mit dem sich auch die Remote gespeicherten Daten verwalten lassen.



FolderSync

Vergleich von Synchronisations-Services in der Cloud

Mit freundlicher Genehmigung des LinuxUser-Magazins wird an dieser Stelle die in Ausgabe 09/2011 (Artikel „Datenwolke“, Seite 25) dargestellte Übersicht verwendet. Eine Spalte (Teamdrive) habe ich dabei ausgelassen, da hier (zumindest derzeit) kein Android-Client existiert.

Tabelle 1.1: Vergleich von Synchronisations-Services in der Cloud (Quelle: LinuxUser)

	Ubuntu One	Dropbox	Spideroak	Wuala	Zumodrive	Min.us
URL	one.ubuntu.com	www.dropbox.com	spideroak.com	www.wuala.com	www.zumodrive.com	minus.com
Gratis-Speicher	5 GByte	2 GByte	2 GByte	1 GByte	1 GByte	5 GByte
Linux-Client	ja	ja	ja	ja	ja	ja
Mac-Client	nein	ja	ja	ja	ja	ja
Windows-Client	in Entwicklung	ja	ja	ja	ja	ja
Mobil-Client	Android, iPhone	Android, iPhone, BlackBerry	Android, Maemo, iPhone	Android, iPhone	Android, iPhone	Android, iPhone, Windows Phone
Sync / Backup	ja / nein	ja / ja	ja / ja	ja / ja	ja / nein	nein / nein
Web-GUI / WebDAV	ja / ja	ja / nein	ja / nein	ja / nein	ja / nein	ja / nein
Sharing / Multi-User	ja / nein	ja / nein	ja / ja	ja / nein	ja / nein	ja / nein
Lokalisierung	ja	ja	nein	ja	nein	nein
Vorteile	Client in Ubuntu bereits enthalten, Integration mit anderen Canonical-Cloud-Diensten	großer Funktionsumfang, weit verbreitet, viele Clients, externe Zusatztools, Webinterface, preiswert bei kostenpflichtigen Versionen	Hervorragendes Sicherheitskonzept, leistungsfähiger Linux-Client, Clients für Android und Maemo	ungewöhnliches Konzept mit verteilter Speicherung, kostenlose und flexible Speichererweiterung mit Option Festplatte tauschen möglich, vorbildlicher Client	Online-Festplatte als Netzwerklaufwerk	einfaches Konzept für einfache Datei-Uploads ohne vorherige Registrierung, Zugriff und Sharing über generische URLs
Nachteile	durchschnittlicher Funktionsumfang, teuer	relativ umständlich	nur in Englisch verfügbar	hohe Systemlast	geringer Funktionsumfang	schwaches Sicherheitskonzept, keine echte Online-Festplatte

1.2 Security

Wie eingangs des Kapitels erwähnt, soll es nun um den Schutz vor Fremdzugriffen gehen. Diesbezüglich möchte ich mehrere Ebenen unterscheiden:

- **Verschlüsselung:** Besonders interessant, wenn Daten auf fremden Servern (Stichwort: Cloud) abgelegt werden. Da es auf selbigen nicht mehr in der Macht des Daten-Eigentümers liegt, den „physikalischen Zugriff“ abzusichern, sichert man auf diese Weise „logischen Zugriff“ ab: Selbst wenn ein „Angreifer“ an die Dateien gelangt, muss er damit noch lange nicht an die Daten (Inhalte) kommen.
- **Zugriffsrechte:** Worauf darf eine App zugreifen? Unschön, wenn da jemand im Hintergrund ungefragt und ungewünscht sämtliche Kontaktdaten „irgendwohin“ verschickt. Oder andere böse Sachen mit unseren Daten anstellt.
- **Malware und Viren:** Sollten eigentlich mit dem vorigen Punkt bereits abgearbeitet sein, werden aber dennoch explizit separat behandelt.
- **Location-Cache:** Noch ein „Datenschnüffler“. Mit ihm ließen sich Bewegungsprofile erstellen („Herr X verlässt werktags fast jeden Vormittag zwischen sieben und acht die Wohnung und geht zu Y (vermutlich Arbeit). Diesen Ort verlässt er dann am späten Nachmittag, und geht zweimal die Woche zu ...“). Solches soll zwar laut offizieller Verlautbarung nicht passieren – aber wie sieht es inoffiziell aus?

Wer sich genauer informieren möchte, welche Schutzmaßnahmen Android selbst anwendet, findet in der Computerwoche einen interessanten Artikel, der sich dem Thema eingehend widmet.



<http://www.computerwoche.de/netzwerke/mobile-wireless/2497291/>

Verschlüsselung

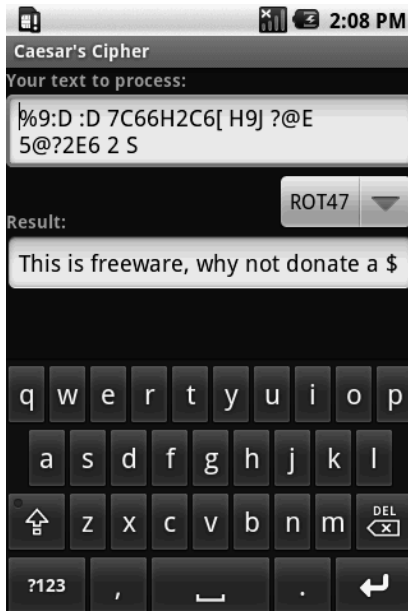
Texte verschlüsseln

Das tat schon Gaius Julius Caesar – weshalb einer der einfachsten Codes auch nach ihm benannt wurde: die Caesar-Verschlüsselung. Die bekannteste Variante aus dieser Reihe trägt den Namen „ROT-13“ – was nicht etwa darauf hinweisen soll, dass Caesar damit die Cleopatra 13 Mal zum Erröten brachte (tat er bestimmt nicht: nach Sueton verwendete Caesar nämlich ROT-4). Vielmehr heißt es: ROTiere jeden Buchstaben 13 Mal – aus „A“ wird also „N“. So wird aus dem Wort „Text“ das etwas schwerer lesbare „Grkg“. Zur Entzifferung verschiebt man die Buchstaben einfach zurück (aus „N“ wird „A“).

Von einer sicheren Kodierung kann hier also beileibe nicht die Rede sein – doch veranschaulicht dies wunderbar, wie Verschlüsselung prinzipiell funktioniert. Genutzt wird es trotzdem – weniger zu Sicherheitszwecken, als vielmehr um z. B. unbeabsichtigtes Lesen

von Spoilern zu vermeiden. Zumindest Geo-Cachern dürfte diese Verschlüsselungsart vertraut vorkommen.

So wird die App **Caesar's Cipher** (Bild 1.30) von ihren Benutzern als hilfreiches und nützliches Tool beim Geo-Caching beschrieben (hier werden Hints kodiert und dekodiert). Oder, wie es ein englischer Kommentar formuliert: *Very useful. Now my teacher has no idea what the gibberish on my paper says.*

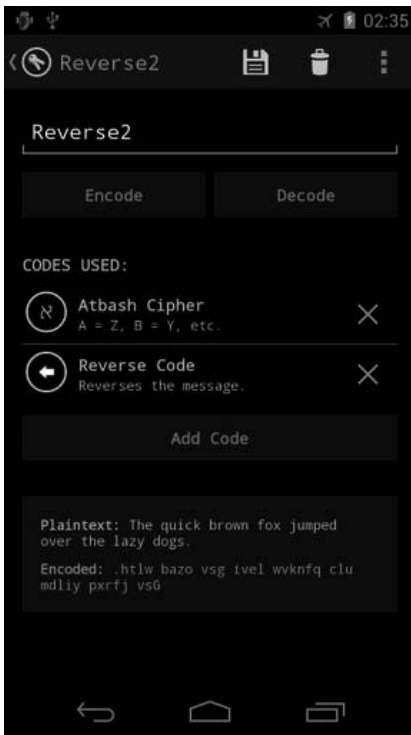


Caesar's Cipher

Bild 1.30: *Caesar's Cipher* verschiebt die Buchstaben im Alphabet

Caesars Code hat natürlich einen großen Haken: War er zu Zeiten des genannten Römers noch relativ sicher, benötigt man heutzutage für das „Knacken“ des Codes wahrscheinlich weniger als eine Sekunde – bedenkt man, dass ein Computer lediglich 26 (bei reinen Großbuchstaben) bzw. maximal 256 Varianten (8-Bit-ASCII) dafür durchspielen muss. So schützt ein reiner Caesar-Code allenfalls vor dem „schnellen Lesen“, nicht aber vor dem Lesen an und für sich.

Doch was galt bereits im Altertum als besonders kompliziert? Da war doch was mit einem Gordischen Knoten, an dessen Auflösung sich viele schlaue und starke Männer vergeblich versuchten. Nach diesem ist offenbar die App **Gordian Secret Code Tool** (Bild 1.31) benannt. Sie nutzt prinzipiell ähnliche Methoden – erlaubt jedoch, diese zu kombinieren. Zugegeben: Ein Caesar-4 mit anschließendem Caesar-9 ergäbe auch nur wieder ROT13. Kombiniert man ihn jedoch beispielsweise mit Vigenère, wird die Sache schon komplexer. Ob der potentielle „Knacki“ deswegen gleich ins Schwitzen kommt, steht natürlich auf einem anderen Blatt...



Gordian Secret
Code Tool

Bild 1.31: Mit dem **Gordian Secret Code Tool** lassen sich verschiedene Algorithmen verknüpfen

Bleiben wir zunächst noch bei den Legenden, machen jedoch einen größeren Zeitsprung über mindestens Tausend Jahre. Damals war es vielen ein Rätsel, was das deutsche Militär da so funkte. Auf Griechisch heißt Rätsel „αίνιγμα“, mit lateinischen Buchstaben schreibt man es „Enigma“ – die Rede ist natürlich von der bekannten Rotor-Schlüsselmachine. Dieses Original benutzte auch eine Kombination, und zwar waren hier mehrere Walzen hintereinander geschaltet, die nach jedem Buchstaben auch noch wie ein Kilometerzähler weiterbewegt wurden. Dies bedeutet, dass sich der Schlüssel nach jedem Buchstaben ändert: Hätte Caesar aus einem *OTTO* vielleicht ein *GLLG* gemacht, wäre bei einer Enigma eher etwas wie *PQWS* dabei herausgekommen. Daran hatten die Alliierten im zweiten Weltkrieg eine ganze Weile zu knabbern.

Wer dieses Feeling einmal nachempfinden möchte, bekommt mit der App **Pocket Enigma Machine** Gelegenheit dazu: Der Entwickler hat hier Bild- und Tonaufnahmen des Originals verwendet, damit sich das Ganze möglichst „echt“ anfühlt.



Pocket Enigma
Machine



Bild 1.32: *Pocket Enigma Machine* ermöglicht es, die legendäre Verschlüsselungs-Maschine nachzuerleben – einschließlich Sound



Crypt Haze

Nah dran waren wir ja nun bereits, doch nun wollen wir uns endgültig der Gegenwart zuwenden. Spricht man heute von einer „sicheren Verschlüsselung“, so fallen Begriffe wie RSA (asymmetrisch) oder DES (symmetrisch). Den Nachfolger des Letztgenannten (AES) macht sich **Crypt Haze** (Bild 1.33) zu Nutze, um Mails und Kurznachrichten zu ver- und entschlüsseln (wozu es natürlich die entsprechenden Zugriffs-Rechte auf Kontakte und SMS anfordert – allerdings auf die allgegenwärtige Internet-Berechtigung verzichtet).

Auch die App **Encrypt It** setzt auf eine 256Bit-AES-Verschlüsselung, und verbindet diese zur Erhöhung der Sicherheit noch mit einem Salt. Diese App verlangt keinerlei Permissions.



Encrypt It

Was aber verwendet der sicherheitsbewusste Mensch von heute, wenn er Nachrichten verschlüsselt oder signiert übertragen möchte? Das Zauberwort heißt GPG. Das „G“ steht hier für „GNU“, und „PG“ für den „Privacy Guard“ – also den Beschützer der Privatsphäre. Hier werden Schlüsselpaare verwendet, bestehend aus einem „privaten“ und einem „öffentlichen“ Schlüssel. Die Namen sagen es bereits: Den einen hütet man wie den eigenen Augapfel, den anderen gibt man frei heraus.

Dank dieses öffentlichen Schlüssels ist nun jeder Anwender von GPG in der Lage, eine Nachricht so zu verschlüsseln, dass sie nur vom Besitzer des zugehörigen privaten Schlüs-

sels wieder dekodiert werden kann. Umgekehrt lassen sich mit dem privaten Schlüssel Nachrichten signieren. Die Echtheit dieser Signatur kann jeder mit dem frei verfügbaren öffentlichen Schlüssel überprüfen.



Bild 1.33: *Crypt Haze* verschlüsselt Mails und Kurznachrichten

Soweit die Theorie und das grobe Prinzip, kommen wir zur Praxis. Die bekannteste App in diesem Segment ist sicherlich **APG** (Bild 1.34). Als Open-Source-Software stellt das Projekt sicher, dass es keine „Hinter-türchen“ geben kann (die würden schnell entdeckt). Durch die Verwendung von Schlüsselpaaren (wie soeben beschrieben) wird darüber hinaus auch eine relativ hohe Sicherheit gewährleistet – zumindest, so lange der private Schlüssel nicht kompromittiert wurde.



APG

Mit der App lassen sich PGP/GPG-Schlüsselpaare verwalten sowie Mails und Dateien verschlüsseln, signieren, entschlüsseln und die Signaturen überprüfen. Unterstützt wird Gmail, aber auch in K9 lässt sich die App integrieren; für andere Apps wird eine API bereitgestellt. Seit Neuestem werden auch Schlüsselservers unterstützt (daher auch die Internet-Berechtigung). 4,5 Sterne bei über 900 Bewertungen bestätigen die Qualität dieser App aus Anwendersicht.



Bild 1.34: APG ver- und entschlüsselt Dateien und Mails. Die App ist kompatibel mit PGP/GPG.

Alternativ bietet sich noch der *OpenPGP Manager* (Bild 1.35) an, dessen Funktionsumfang annähernd dem von APG entspricht – wenn man die K9-Integration sowie die API abzieht. Auch hier ist eine vollständige Schlüsselverwaltung (wie abgebildet) enthalten, einschließlich der Unterstützung von Keyservern.



OpenPGP Manager



Bild 1.35: Auch *OpenPGP Manager* versteht sich auf den Umgang mit den Schlüsseln



Eine Übersicht mit Apps zum Thema Textverschlüsselung findet sich *im Forum bei AndroidPIT*.

<http://www.androidpit.de/de/android/forum/thread/435104/>

Passwort-Safes

Ein ganz spezieller Fall von „kurzen Texten“, die es um jeden Preis abzusichern gilt, sind sicher Passwörter und PIN-Codes. Eine App, der ich solche Daten anvertraue, sollte möglichst mein Handy auch nicht verlassen – sonst bestünde ja immer die Möglichkeit, dass sie diese sensiblen Daten (von mir unbemerkt) an Dritte weiterreicht. Zum Glück sehen das viele Entwickler ähnlich – anderen ist hingegen beispielsweise wichtiger, auch ein „Backup“ in der Cloud ablegen zu können. Das wäre aus meiner Sicht allerdings, wenn überhaupt, Aufgabe einer anderen App aus anderem Hause – ich bin halt ein wenig vorsichtig. Daher werde ich mich hier auf Apps beschränken, die über keine eigene „Internet-Berechtigung“ verfügen.

Da wären zum Beispiel die PINs von EC- und Kreditkarten. Der Eine oder die Andere kennt vielleicht noch diese kleinen „Geheimkärtchen“, auf denen man sich diese in der Regel vierstelligen Zahlencodes „verschlüsselt“ notieren kann – und genau dieses Prinzip greift **PIN'r** (Bild 1.36) auf: Die PINs werden in einer Tabelle voller Zufallszahlen versteckt.



PIN'r

Bild 1.36: Pin'r versteckt PIN-Codes – wie etwa die von EC-Karten

Nur wer das Geheimwort kennt, findet die richtige Kombination wieder. Dumm für den Schnüffler: Jedes beliebige „Geheimwort“ liefert passende Zahlencodes, mit „Passwort erraten“ ist es also auch nicht ganz so einfach ...



Password Safe

Doch oftmals geht es um mehr als nur PINs: Zugangsdaten für Foren und Websites, Kreditkartendaten, Mailkonten, Lizenzschlüssel für Software ... Zahlreiche Daten sind sensitiv genug für einen Passwort-Safe. Da bieten sich Apps wie beispielsweise **Password Safe** (Bild 1.37) an. Für jeden Anwendungsbereich lassen sich hier Vorlagen (Templates) definieren: Für ein Mailkonto benötigt man in der Regel drei bis vier Felder (Name, Mail-Adresse, Passwort sowie ggf. zugehörige Webseite) – für weitere Mailkonten sind es die gleichen vier Felder. Wie es im Fall von Kreditkarten aussehen könnte, zeigt der Screenshot. Einige Templates bringt die App gleich mit, weitere kann man selbst erstellen (bzw. die vorhandenen entsprechend anpassen). Jeder Vorlage lässt sich darüber hinaus auch ein Icon zuordnen, was die Erkennung vereinfacht. Bei Erfassung der Daten wählt man dann einfach das jeweilige Formular (also die Vorlage) aus und füllt die Daten in die Felder; selbst jetzt lassen sich bei Bedarf noch zusätzliche Felder hinzufügen.

The screenshot shows the 'Password Safe' app interface. At the top, there's a status bar with a download icon, signal strength, battery level, and the time 22:15. Below the app title 'Password Safe', the section is titled 'Password Record'. The form contains the following fields: 'Title' with the value 'credit card' and a card icon; 'Category' with a dropdown menu showing 'Cards'; 'Card Provider' with the value 'Citibank'; 'Card Type' with the value 'VISA'; 'Card Number' with the value '2486-7465-1324-6890'; 'Expiration Date' with the value '2012-12-13' and a calendar icon; 'PIN' with the value '479'; and 'Password' with the value '939546'. At the bottom, there are four buttons: 'Add Field' (plus icon), 'Save' (floppy disk icon), 'Delete' (X icon), and 'Back' (left arrow icon).

Bild 1.37: Mit **Password Safe** lassen sich viele vertrauliche Informationen verwalten

Da so eine Datensammlung schon einmal etwas größer ausfallen kann, ermöglicht **Password Safe** auch eine Einteilung in Kategorien; die Darstellung erfolgt hier in einer Baumstruktur, in der man sich leicht zurechtfinden kann. Davon kann man sich in einer Gratis-

Version der App zunächst überzeugen – die erfassten Daten lassen sich in die für ca. zwei Euro erhältliche Vollversion übernehmen, die dann auch einen Export/Import im CSV-Format ermöglicht.

Und bevor ich es zu erwähnen vergesse: Damit die Daten vor fremden Blicken geschützt sind, werden sie mit 128Bit-AES verschlüsselt gespeichert. Wem das noch nicht ausreicht, der kann einen Blick auf **Passman** werfen. Hier gibt es zusätzlich eine „Selbstzerstörung“: Nach einer konfigurierbaren Anzahl von Fehlversuchen bei der Eingabe des Master-Passwortes werden sämtliche erfassten Daten automatisch gelöscht. Ein etwaiger Handy-Dieb hat somit wenig Chancen – und man selbst hat ja hoffentlich ein Backup der Datenbank an anderer Stelle (z. B. auf dem PC) abgelegt.



Passman

Natürlich gibt es noch jede Menge weiterer Apps zu diesem Thema. Solche, die den beschriebenen ähneln – aber auch andere, die aber zumeist die Berechtigung für den Internet-Zugriff (meist für eine Speicherung der verschlüsselten Datenbank bei Dropbox & Co) einfordern.



<http://www.androidpit.de/de/android/forum/thread/410909/>

Dateien und Verzeichnisse

Da fällt einem sicher als erstes **TrueCrypt** ein – was für Android noch nicht so lange verfügbar ist; allenfalls konnte man **TrueCrypt**-Container auf dem Androiden ablegen, um so einen „portablen, sicheren Speicher“ bei der Hand zu haben (wie man das für besonders große Container umsetzt, beschreibt ein Artikel bei AndroidPIT).



<http://www.androidpit.de/de/android/forum/thread/407709/>

Vom Verhalten am Nächsten kam dem bislang der **LUKS Manager** (Bild 1.38), der AES-verschlüsselte Container verwaltet. Diese können wie andere Dateisysteme eingebunden werden und stehen dann ebenso anderen Apps zur Verfügung. **LUKS** kümmert sich sowohl um die Erstellung/Entfernung als auch das Einbinden/Aushängen der entsprechenden Container.



LUKS Manager

Die App ist zwar gratis – doch sind die Hürden für den „einfachen Anwender“ ein wenig hoch. So wird nicht nur root-Zugang inkl. der App **BusyBox** vorausgesetzt – auch ein passender Kernel, der DM_CRYPT und „Loopback“ unterstützt, muss vorhanden sein (beides Dinge, die auf die meisten Standard-Kernels/Standard-ROMs nicht zutreffen), womit **LUKS** für die meisten Android-User leider als Option ausfällt.





Bild 1.38: LUKS Manager verschlüsselt mit AES



Eds

Alternativ gibt es seit ein paar Monaten **Eds**. Und diese App arbeitet mit *TrueCrypt*-kompatiblen Containern. Auch ist von den bei *LUKS* genannten Hürden hier an keiner Stelle zu lesen. Sogar Dropbox-Support ist direkt aus der App (Vollversion) heraus möglich, sodass man seine verschlüsselten Container in der Cloud ablegen kann – das mindert die Bedenken gegen „Schnüffler im Netz“, da diese ja in den Container nicht hineinschauen können.

Eds gibt es in einer Gratisversion (ohne Dropbox-Support und mit minimalen Rechte-Anforderungen, u.a. kein Netzwerkzugriff) sowie in einer Vollversion für derzeit ca. fünf Euro. Beide Varianten sind sehr gut bewertet.



SecretVault

Womit wir zu **SecretVault** (Bild 1.39) als nächster Alternative kommen. Anders als bei *LUKS* handelt es sich hier nicht um Open Source – wodurch die auch in der Kaufversion geforderte Berechtigung zum Internet-Zugriff manch einem ein wenig Bauchschmerzen bereiten dürfte. Selbst in der Pro-Version lässt sich nur ein einziger Container verwenden, der mit der App selbst im Basisverzeichnis der SD-Karte erstellt wird. Wurde dieser Container eingebunden, steht er transparent als Verzeichnis im System zur Verfügung, bis die App selbst beendet oder der Container aus der App heraus geschlossen wird.

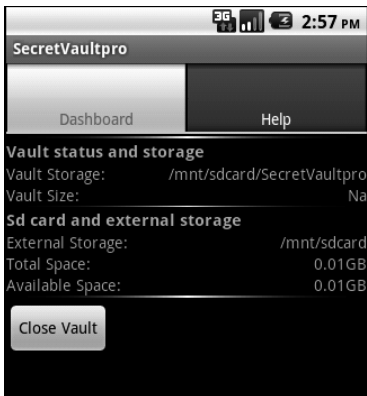


Bild 1.39: *SecretVault* kann genau einen verschlüsselten Container verwalten, der sich anderen Apps transparent zur Verfügung stellen lässt

Detailliertere Informationen, eine Reihe weiterer Screenshots sowie eine kurze Beschreibung des Umgangs mit *SecretVault* finden sich im *Blog der App*.

Damit wäre der Vorrat an „transparenten Container-Apps“ allerdings leider bereits erschöpft. Es verbliebe aber noch die Möglichkeit, Dateien und Verzeichnisse separat zu verschlüsseln. Der Favorit hierfür dürfte **Droid Crypt** (Bild 1.40) heißen und verschlüsselt wahlweise einzelne Dateien oder ganze Ordner (auf Wunsch gleich rekursiv) mittels AES. Auch diese App vermag es, sich als Mittler zwischen den Apps und den verschlüsselten Daten zu betätigen – und so eine gewisse Transparenz zu ermöglichen. Der Anwender muss also nicht erst die benötigten Daten von Hand entschlüsseln, um sie mit einer App zu bearbeiten (und nicht vergessen, sie hinterher wieder zu verschlüsseln). Wer mag, kann zusätzlich eine Datenkompression vornehmen lassen: Auf diese Weise spart man zusätzlich Speicherplatz.



<http://secretvaultpro.blogspot.de/>



Droid Crypt



Bild 1.40: *Droid Crypt* verschlüsselt Dateien und Verzeichnisse mit AES

Interessant ist auch die Wahl des Passwortes. Oder auch nicht – denn ein solches ist nicht zwingend erforderlich. Stattdessen lässt sich auch ein „Schwenkmuster“ verwenden.



<http://www.androidpit.de/de/android/forum/thread/411330/>

Die Testversion von *Droid Crypt* verlangt noch den Zugriff auf's Internet für Werbeeinblendungen; nach 60 Tagen Testzeitraum ist sie darüber hinaus auf die Ver- und Entschlüsselung von einzelnen Dateien beschränkt. Beides gilt natürlich nicht für die Vollversion, die man bereits für ca. zwei Euro erwerben kann. Eine kurze Liste weiterer möglicher Kandidaten für die Ver-/Entschlüsselung von Dateien und Verzeichnissen findet sich **im AndroidPIT-Forum**.

Ab Android 3.0 (aka *Honeycomb*) auf Tablets bzw. 4.0 (aka *Ice Cream Sandwich*) auch für Smartphones (für Besitzer des Samsung Galaxy S2 bereits ab Android 2.3 *Gingerbread*) werden all diese Umwege für die meisten Anwender unnötig werden: Hier ist eine Verschlüsselung des gesamten Gerätes von Haus aus mit dabei. Zum Einsatz kommt dafür dm-crypt mit 128-Bit AES-Verschlüsselung. Der Anwender muss dann bei jedem Bootvorgang das zugehörige Kennwort zur Entschlüsselung des Dateisystems eingeben – ab diesem Zeitpunkt stehen die Daten dann allerdings unverschlüsselt zur Verfügung.

Apps mit Passwort absichern

Viele Gründe kann es geben, warum man so etwas tun möchte: Etwa wenn man sein Handy „mal eben“ einem Kollegen „nur für einen kurzen Anruf“ übergibt. Oder es einem Freund „für ein paar Tage“ borgt, während dessen Telefon sich „in Reparatur“ befindet. Darüber hinaus kann es sich als sinnvoll erweisen, seinem Kind die Nutzung des Smartphones zwar prinzipiell nahezubringen – aber dennoch nicht zuletzt aus Sicherheitsgründen etwas einzuschränken.



Child App
Protector

Im letztgenannten Fall bietet sich insbesondere **Child App Protector** (Bild 1.41) mit einigen nützlichen Einstellungen an. Eine davon zeigt die Abbildung bereits: Die Nutzung bestimmter Apps (etwa Spiele oder Chat-Apps) lässt sich zeitlich limitieren – damit sich der „Zögling“ nicht ausschließlich damit beschäftigt. Aber vielleicht möchte man bestimmte Dinge ja komplett abschalten – oder sicherstellen, dass gewisse Einstellungen nicht verändert werden? Auch das stellt die App nicht vor Probleme: Ausgewählte Apps lassen sich gegen einen Start schützen, solange *Child App Protector* aktiv ist (hier sollte man einen etwaigen Task-Killer nicht vergessen). Schmanke! Man kann je App eine „alternative App“ festlegen. Wird nun versucht, die gesperrte App zu starten – startet stattdessen die Alternative (auch „erzieherische Maßnahme“ genannt). Zu guter Letzt lässt sich auch ein Backup des Homescreens anfertigen bzw. bei „ungewollten Änderungen“ an selbigem wiederherstellen.

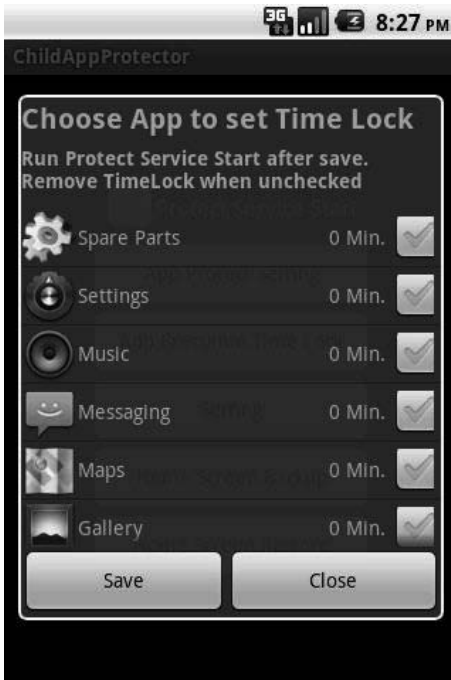


Bild 1.41: Child App Protector erlaubt es einzuschränken, worauf das Kind Zugriff hat – und wie lange

Damit wären eigentlich alle Fälle abgedeckt. Aber dennoch gibt es einige Alternativen, die genannt werden möchten. Weniger in Sachen Kinderschutz: Das Thema ist ja vielmehr der Schutz von Apps. Und da hat sich **App Schutzeinrichtung** (oder besser deren Entwickler) etwas besonders Nettes einfallen lassen: Versucht jemand, eine geschützte App zu starten, so sieht er so etwas, wie in Bild 1.42 zu sehen ist. Es wird ein Systemfehler vorgegaukelt, so als sei die betreffende App halt einfach kaputt. Dem unberechtigten Nutzer wird also weisgemacht: „Du brauchst es gar nicht weiter probieren, das Ding ist im Eimer.“



App Schutz-einrichtung

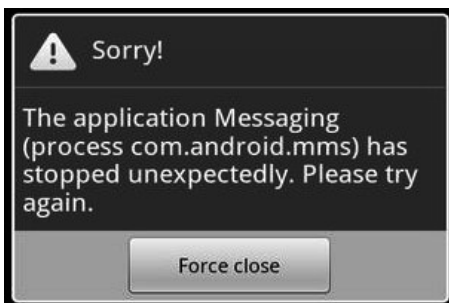


Bild 1.42: App Schutz-einrichtung gaukelt beim Zugriff auf geschützte Apps einen Systemfehler vor

Application
Protection

Als weitere Alternative wäre noch **Application Protection** zu nennen – von fast achttausend Anwendern mit durchschnittlich 4,4 Sternen bedacht, kann diese App ja nicht schlecht sein. Apps lassen sich hier wahlweise mit einem Sperrmuster oder einem Code schützen. Dabei wird davon ausgegangen: Wurde der korrekte Code einmal eingegeben, handelt es sich wohl auch um den „rechtmäßigen Besitzer“ – bis zur nächsten „Scharfschaltung“ (die bei Neustart des Gerätes automatisch eintritt) bleibt man daher von weiteren Anfragen verschont. Dies lässt sich konfigurieren und kann so pro App oder global aktiviert werden.

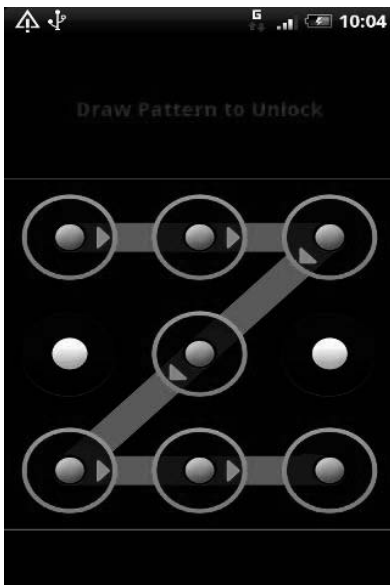


Bild 1.43: *Application Protection* schützt Apps vor unbefugtem Zugriff

Übrigens: Wird bei dieser App zehn Mal ein falscher Code eingegeben, verschickt sie automatisch eine Mail an die in der App konfigurierte Adresse. Der Beschreibung nach lässt sich darauf schließen, dass diese Mail auch den korrekten Sperr-Code enthält – gut für den Fall, dass man ihn selbst einmal vergessen hat. Für diesen Fall lässt sich allerdings auch ein Merksatz hinterlegen.



<http://www.androidpit.de/de/android/forum/thread/435325/>

Wem nun diese kurze Zusammenstellung noch nicht genügt, der findet in der Übersicht bei AndroidPIT noch weitere Kandidaten.

Zugriffsrechte

Permissions werden oftmals zu wenig beachtet oder falsch interpretiert. Nur wenige scheinen ihre Bedeutung überhaupt *richtig* zu verstehen und korrekt mit ihnen umzugehen – das betrifft nicht nur die Anwenderseite, sondern ebenso die Entwickler. Wofür sind diese „Permissions“ eigentlich gut, was nützen sie? Um das zu verstehen, müssen wir einen kurzen Blick hinter die Kulissen werfen.

Android baut bekanntermaßen auf Linux auf. Hier verwaltet das System u. a. Benutzer und Benutzergruppen, um die „Eigentumsverhältnisse“ zu klären: Auf die Daten eines anderen Benutzers kann somit nicht ohne Weiteres zugegriffen werden. Während unter Linux ein Benutzer vereinfacht betrachtet einer am Rechner angemeldeten Person entspricht, teilt Android jeder App eine eigene Benutzer-ID zu. Somit kommt eine App in der Regel nicht ohne Weiteres an die Daten der anderen Apps heran. Ist sie mit keinerlei expliziten Permissions ausgestattet, kann sie nur „völlig ungefährliche“ Aktionen ausführen: etwas auf dem Bildschirm anzeigen, eigene Daten speichern, und ähnliche Dinge.

Für den Zugriff auf Spezielleres muss der Entwickler seine App entsprechende Permissions anfordern lassen – und zwar bereits bei der Installation (im Nachhinein ist dies auf normalen Wegen nicht mehr möglich). Am bekanntesten ist hier sicher der Zugriff auf das Internet. Aber auch der Zugriff auf persönliche Daten wie Kontakte und Termine, das Benutzen von Hardware-Elementen wie Kamera und Vibrator oder gar das Anpassen von Systemeinstellungen bedarf expliziter Genehmigung. Eine Auswahl verfügbarer Permissions und ihrer Bedeutung findet sich im Anhang *Google Permissions – und was sie bedeuten*.

Wo liegen nun die größten Fehler im Umgang mit diesen Permissions?

Bei Anwendern am ehesten darin, dass sie sie häufig ohne genaueres Hinschauen abnicken, weil sie die App ja haben wollen. Dies liegt nicht zuletzt in einem Schwachpunkt des Android-Systems begründet: „Alles oder nichts“ – entweder alle geforderten Permissions werden akzeptiert, oder die fragliche App kann halt nicht installiert werden. Wünschenswerter wäre es hier, einzelne Permissions gezielt ausklammern zu können. Das würde zum einen die Anwender motivieren, sich überhaupt einmal mit ihnen zu beschäftigen – und zum anderen so manch einer Malware die Grundlage entziehen. Möglich ist dies derzeit nur, sofern man über root-Rechte verfügt oder die entsprechenden Apps modifiziert.

Bei Entwicklern ist der Fehler häufig, dass sie zu viele Permissions anfordern. Entweder aus Unwissenheit, aus Bequemlichkeit („so kann ich nichts vergessen“) oder mit dem Hintergedanken: „Wenn das später mal gebraucht wird, und ich es erst dann hinzufüge, bekomme ich nur wieder böse Kommentare.“

Was sollte man also im Umgang mit Permissions besser beachten?

Der Anwender sollte sich vor der Installation einer App genauer fragen: Ergeben die geforderten Permissions für die gebotene Funktionalität Sinn? Sicher benötigt eine SMS-App

Zugriff auf die Kurznachrichten und muss selbige auch senden können (auch wenn dies natürlich Kosten verursachen kann). Sie muss aber weder Telefonanrufe tätigen noch den Netzwerkstatus ändern können. Eine Wallpaper-App wiederum hat an den Kurznachrichten gar nichts zu suchen. Die Alarmglocken läuten in den lautesten Tönen, wird etwa eine Permission zur Installation weiterer Packages gefordert (was allerdings i. d. R. ins Leere laufen dürfte, da an dieser Stelle weitere Sicherheitsmaßnahmen des Systems greifen).

Sicher gibt es hier Grenzfälle: Besagte SMS-App könnte das Internet zum Versenden kostenloser/kostengünstiger SMS über entsprechende Web-Services nutzen. Sie benötigt natürlich auch Zugriff auf die Kontakte (wohin schickt man wohl SMS?). Und spätestens hier taucht die Frage auf: Könnte sie dann eine Kopie der kompletten Kontaktliste an eine dubiose Website verschicken? Die Antwort: Ja, sie könnte – sie hat schließlich sowohl vollständigen Zugriff auf die Kontakte (lesend genügt ja) als auch auf das Internet. Da kann man wohl nichts machen? Oh doch: Auf den Entwickler zugehen, damit er sich den folgenden Abschnitt zu Herzen nimmt:

Entwickler sollten natürlich ihre Apps nur die Permissions anfordern lassen, die wirklich benötigt werden. Das lässt auch ihre Apps vertrauenswürdiger aussehen. Bei „gefährlichen Kombinationen“ wie „Kontaktdaten lesen & Internet“ sollte, sofern möglich, die Auslagerung in ein AddOn in Erwägung gezogen werden. Positives Beispiel: **Locus Maps**. Sicher ist hier ein Zugriff auf die Kontaktdaten sinnvoll: um Adressen auf der Karte anzeigen zu können. Für den Download von Kartenmaterial wird allerdings der Zugriff auf das Internet benötigt. Der Entwickler entschied sich also, den Kontaktdaten-Zugriff in ein eigenes AddOn (**Locus - addon Contacts**) auszulagern. Somit sind die Permissions der Kern-App wieder „unanständig“ – und dem Anwender steht es frei, die App mit oder ohne diese „Bequemlichkeit“ des Zugriffs auf die Kontaktadressen zu nutzen. Vorbildlich, Menion! Mögen sich viele Entwickler daran ein Beispiel nehmen!

Permissions überprüfen

Leider kommt es oftmals vor, dass man die Liste der geforderten Permissions vor der Installation eben *nicht* (oder *nicht genau*) gelesen hat – obwohl man es sich fest vorgenommen hatte. Oder dass die Einsicht erst beim Lesen dieses Buches kam – und natürlich bereits allerhand „unbedacht Installiertes“ auf dem Androiden „herumliegt“. In beiden Fällen ist eine nachträgliche Überprüfung geboten.



RL Permissions

Was nicht immer einfach ist: Bei den vielen unterschiedlichen Permissions ist nicht immer klar, was sie eigentlich bedeuten. Wer hier einmal alles ein wenig genauer abklopfen will, findet unter Umständen in **RL Permissions** (Bild 1.44) das Werkzeug seiner Wahl. Mit dieser App lassen sich zum einen alle Apps auflisten, die eine gewählte Permission verlangen – oder umgekehrt alle Permissions, die eine bestimmte

App verlangt. Dabei wird zu den Permissions auch jeweils eine Erklärung geliefert, was sie bedeuten. Ob von ihnen eine potenzielle Gefahr ausgeht, besagt auch die kleine jeweils neben ihnen angezeigte Ampel. Auch hier heißt „rot“ nicht gleich, dass eine App „böse“ ist – sondern lediglich, dass sie es potenziell sein *könnte*.



Bild 1.44: *RL Permissions* gibt einen Überblick über die Berechtigungen installierter Apps

Es gibt natürlich noch weitere Apps, die Ähnliches tun – einige davon sind in einem Artikel bei AndroidPIT näher vorgestellt.

Permissions überwachen

Eine echte Überwachung einschließlich der Möglichkeit, einer App bei „unbefugtem Zugriff“ auf die Finger zu hauen – das ist ohne *root* leider nicht möglich. Denn dazu bedarf es ja eines Zugriffs auf die Aktivitäten der jeweiligen App – eine Sache, die das Berechtigungssystem so nicht erlaubt. Schade daher, dass die entsprechende Möglichkeit nicht von Haus aus ins System integriert ist; eine solche Schutzfunktion ist aus meiner Sicht unerlässlich.

Dass ich mit dieser Meinung nicht allein dastehe, zeigt sich auch darin, dass einige Entwickler sich der Sache bereits angenommen haben. So erlaubt etwa das Custom-ROM von Cyanogen, Apps einzelne Permissions zu entziehen. Und es gibt die App **LBE Privacy**

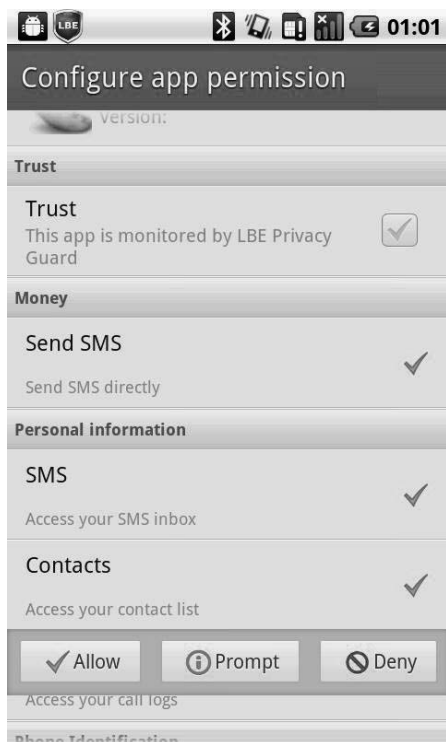


<http://www.androidpit.de/de/android/forum/thread/425974/>





Guard (Bild 1.45), die dies dynamisch erlaubt. Die App teilt auch in der Notification Area mit, wenn eine neue App installiert wurde – und bietet die Konfiguration einiger Permissions an: So lässt sich beispielsweise der von ihr gewünschte Zugriff auf Netzwerk und Systemlogs unterbinden, während beim Zugriff auf Kontakte eine Rückfrage erfolgen soll („Die App XYZ möchte... Darf sie das?“).



LBE Privacy Guard

Bild 1.45: *LBE Privacy Guard* versorgt Apps mit Fake-Daten

Die Voreinstellungen lauten hier: Nachfragen. Dabei erfolgt nach 15 Sekunden ein „Timeout“, falls man die Abfrage verpasst (etwa weil die App den Zugriff im Hintergrund, bei ausgeschaltetem Display, tätigte). In diesem Fall wird der entsprechende Zugriff unterbunden. Und das scheinbar recht intelligent, denn mir ist dabei noch keine einzige App abgestürzt! Ich vermute daher, dass *LBE* hier Fake-Daten erzeugt: Das Adressbuch ist dann beispielsweise leer, das Internet gerade nicht verfügbar und die IMEI ein Fantasiewert.



Privacy Blocker

Hat man ohne *root* denn wirklich nicht die geringste Chance? Ganz so ist es zum Glück nicht, denn es gibt beispielsweise **Privacy Blocker**. Ohne *root* kann auch diese App natürlich nicht „in den laufenden Betrieb“ eingreifen – daher ist das Vorgehen hier ein vollständig anderes: Der Benutzer wählt zunächst die gewünschte App (die mit den unerwünschten Permissions) aus. *Privacy Blocker* greift sich daraufhin die

.apk-Datei dieser App, nimmt sie auseinander und präsentiert dem Anwender die Liste der von ihr geforderten Permissions. Hier lassen sich nun „unerwünschte“ Permissions auswählen – und schließlich wird eine neue .apk-Datei erzeugt, die eben diese nicht mehr verlangt. Selbige kann man nun installieren.

Klingt soweit eigentlich ganz gut, nur hat die Sache zwei „kleine“ Haken: Zum einen eignet sich die so erzeugte .apk-Datei nicht für das Update einer bereits installierten Version (die Signatur hat sich geändert – Android hält es also für eine andere App, die dummerweise nur gleich heißt). Zum anderen wird die App nun mit großer Wahrscheinlichkeit abstürzen, wenn sie auf eine Funktionalität zugreift, für die sie nun keine Permission mehr hat: Da der Entwickler (mit Recht) davon ausgehen konnte, dass ihm der Zugriff erlaubt wird, hat er diesen „Zugriffsfehler“ wahrscheinlich nicht abgefangen. Bei einem „bösen“ Zugriff ist dies mit Sicherheit die bessere Alternative. War der Zugriff aber doch funktional erwünscht, weiß man nun zumindest Bescheid, wozu diese Permission benötigt wird – und installiert entweder die Originalversion oder baut sich mit *Privacy Blocker* eine weniger restriktive Fassung.

Die App ist im Playstore für ca. anderthalb Euro verfügbar. Eine Gratis-Testversion gibt es ebenfalls; diese beschränkt sich jedoch auf die Anzeige, geänderte .apk-Dateien lassen sich damit nicht erstellen.

Firewalls

Auch sogenannte „Personal Firewalls“ fallen in die Rubrik „Zugriffsrechte“ – dienen sie doch dazu, den Zugriff auf bestimmte Dinge zu beschränken. Wieder einmal gilt die übliche Einschränkung: „Ohne root sich nichts tut“, denn so etwas greift tiefer ins System ein.

Um den Bereich „Bluetooth“ kümmert sich **Bluetooth Firewall** – und benötigt dafür ausnahmsweise keinen *root*. Und was tut so eine Firewall? Sie sperrt alles Unerwünschte aus.

Und so schlägt die *Bluetooth Firewall* beispielsweise Alarm, wenn eine App mit Bluetooth-Fähigkeiten installiert bzw. aktualisiert wurde oder Bluetooth-Aktivitäten starten will, aber auch, wenn jemand von außen per Bluetooth zugreifen möchte. Außerdem ermöglicht sie einen Bluetooth-Scan (welche Bluetooth-Geräte sind in Reichweite?), protokolliert alle Bluetooth-Aktivitäten und gibt dem Anwender die Möglichkeit, ausgewählte Bluetooth-Geräte als „vertrauenswürdig“ einzustufen.

Für die Internet-Verbindungen hingegen ist **DroidWall** (Bild 1.47) zuständig. Genau genommen handelt es sich hier nur um eine Eingabemaske zur Erfassung von Regeln – die eigentliche Arbeit macht *iptables*, welches hoffentlich bereits auf dem Androiden installiert ist –, denn dies ist natürlich Voraussetzung für die Funktionalität, aber leider nicht auf jedem Androiden gegeben – sollte *iptables* nicht vorhanden sein, hilft daher nur ein Custom-ROM.



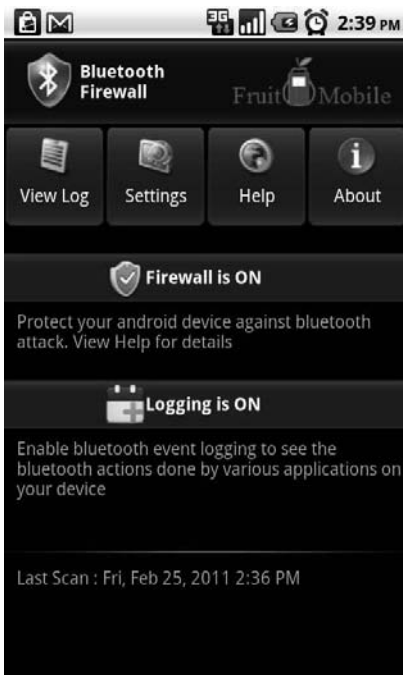


Bild 1.46: *Bluetooth Firewall* schützt die Bluetooth-Verbindungen

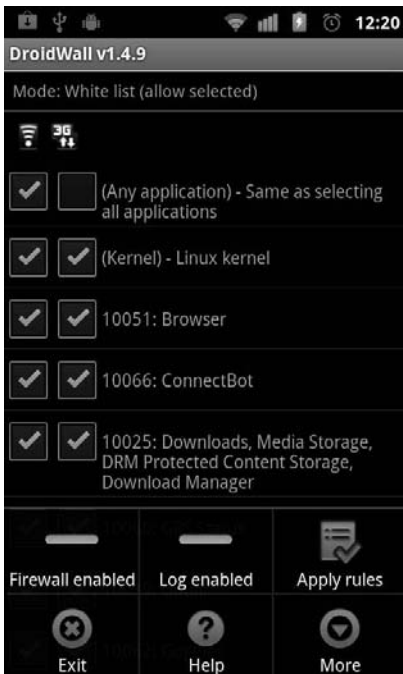


Bild 1.47: Mit *DroidWall* lässt sich festlegen, welche App ins Netz darf



Ein schönes Feature von *DroidWall* ist, dass sich der Zugriff getrennt nach Netzwerk-Interface steuern lässt: So kann man einer datenhungrigen App die Nutzung des mobilen Internets verbieten und sie auf WLAN-Verbindungen beschränken, während man (vermeintlichen) „Schnüfflern“ den Netzzugang komplett untersagt.



DroidWall

Übrigens zeigt der Screenshot noch etwas anderes recht eindrücklich: Die Zahlen vor den Namen der aufgeführten Apps bezeichnen die User-ID derselben. Man sieht, was ich eingangs bereits beschrieb: Unter Android bekommt jede App eine eigene User-ID. Und über diese kontrolliert auch *DroidWall* den Netzzugriff.

Location-Cache

War da nicht was? Legte da nicht wer Bewegungsprofile seiner Nutzer an? Potenziell möglich wäre so etwas auch unter Android: Möchte man hier beispielsweise die „netzwerkbasierte Standortermittlung“ aktivieren, erfolgt prompt der Hinweis, dass man dann auch die damit verbundenen Informationen „freiwillig“ an Google weitergibt. Und spätestens seit Android 2.2 heißt es auch hier: „Alles oder nichts“. Also keine „netzwerkbasierte“ (und damit Akku-schonende) Lokalisierung, ohne „Big Brother“ zu informieren, wo man ist.

Der Zusammenhang dürfte wahrscheinlich sein, dass Google gern über „neue“ oder „umgezogene“ Zellen (Mobilfunk und WLAN) informiert sein möchte, um diese bei weiteren Ortungs-Anfragen nutzen zu können – schließlich erfolgt die Zuordnung des Standortes ja über eine von Google bereitgestellte Datenbank. Einen faden Beigeschmack hinterlässt dies trotzdem – nicht zuletzt, weil der Grund dafür gar nicht mitgeteilt wird. Man darf also raten.

Hat man diesen Ortungsdienst nun aktiviert, werden alle Ortungsdaten „gepuffert“, d. h. in einem Zwischenspeicher (auch „Cache“ genannt) abgelegt. Ab und an kommt dann ein kleines Google-Dienerlein vorbei, packt den Inhalt zusammen und verschickt die Daten in Googles Rechenzentrum. Ist also nichts im Cache, wird auch nichts verschickt – einen Sachverhalt, den **Location Cache** (Bild 1.48) zu unseren Gunsten ausnutzen kann.



Location Cache

Die rot beschrifteten Buttons lassen es unschwer erkennen: Die App kann den Cache leeren und sogar blockieren. In letzterem Fall wird er sozusagen „schreibgeschützt“, sodass keine neuen Daten darin abgelegt werden können. Das ist effektiv: Die netzbasierte Ortung funktioniert weiterhin, die Daten-Krake aber bleibt ungefütert. Dafür dauert die erste Anzeige auf der Karte dann gegebenenfalls ein wenig länger, da die Daten ja nicht dem Cache entnommen werden können.



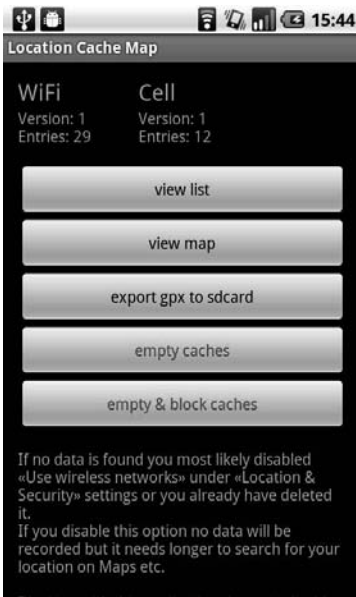
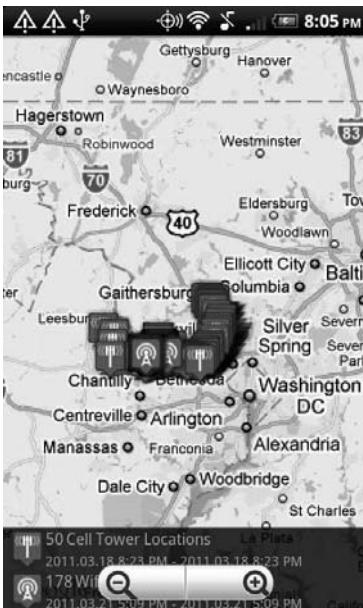


Bild 1.48: *Location Cache* zeigt nicht nur die gecachten Daten an, sondern kann den Cache auch sperren



Eine weitere Möglichkeit hat die App mit dem **Android Location Cache Viewer** gemeinsam: Bei gefülltem Cache können uns beide Apps mitteilen, wo wir in letzter Zeit gewesen sind. Dabei stellt man erfreulicherweise fest, dass der Füllstand des Caches recht begrenzt ist – und zwar auf 50 Mobilfunk-Zellen sowie 200 WLAN-Netze.



Android Location
Cache Viewer

Bild 1.49: *Location Cache Viewer* kann die gespeicherten Ortsdaten lediglich anzeigen



Beide Apps können die im Cache gespeicherten Locations übrigens auf der Karte anzeigen und erlauben auch den Export der Daten im GPX-Format, damit wir zumindest unsere eigenen Bewegungs-Profile erstellen können. Ebenfalls für beide Apps gilt wieder die übliche Einschränkung beim Eingriff in System-Internia: root-Zugang zum Gerät ist Grundvoraussetzung.

Malware und Viren

Zu diesem Thema gibt es ja fast jede Woche (zumindest gefühlt) einen Artikel in den News. In Bild-Deutsch gesprochen: „140% aller Android-Apps sind mit Malware und Viren verseucht!“. Meist kommen diese Warnungen von wohlbekannten Firmen aus dem Sicherheitssektor mit Namen wie Kaspersky oder McAfee. Moment, woher kommen uns diese Namen bekannt vor? Richtig: Diese Firmen bestreiten ihren Umsatz mit dem Verkauf von Anti-Virus- und Anti-Malware-Produkten. Da ist sicher die Frage erlaubt: Wollen die nur den Umsatz ankurbeln – oder ist an den Meldungen etwas dran?

Was macht denn diese böse Malware? Als Beispiel nennt McAfee eine Kalender-App, die heimlich Premium-SMS verschickt. Was haben wir jedoch bereits im Abschnitt über *Zugriffsrechte* gelernt: Vor der Installation prüfen, ob Berechtigungen sinnvoll sind. Wo hat bitte die Permission zum SMS-Verschicken bei einer Kalender-App Sinn? Eigentlich hätte sie bereits an der Stelle auffallen müssen. Bei vielen der anderen genannten Beispiele verhält es sich ähnlich; es kam mir bislang kein Beispiel unter, das nicht in dieses Muster gepasst hätte. Und leider gehen die Sicherheits-Apps der namhaften Hersteller, was das Anfordern von Permissions betrifft, nicht gerade mit gutem Beispiel voran – schon mehrfach musste ich dabei denken: „Liebe Leute, nach Euren eigenen Vorgaben dürfte ich Eure App gar nicht installieren.“

GMV

Damit bin ich bei einem meiner Lieblings-Themen angekommen: Seit ich **GMV** zum ersten Mal in einem Post bei AndroidPIT und dann auch im *Inoffiziellen Android-Handbuch* genannt habe, bekam ich des Öfteren Anfragen, wo man diese Android-App denn herunterladen könne. Auch Google-Suchanfragen nach „GMV App Android“ fanden schon den Weg auf meinen Server. Dabei braucht man doch nur dem Link zu folgen...



GMV

Also noch einmal im Klartext: Bei GMV handelt es sich *nicht* um eine Android-App. GMV sollte im *biologischen Speicher* (auch als „Brain 2.0“ bekannt) *vorinstalliert* sein. Die Abkürzung steht nämlich für „Gesunder Menschenverstand“. Und den hat doch hoffentlich jeder, zumindest in gewissem Umfang. Natürlich kann man sich alle möglichen Anti-Viren- und Anti-Malware-Apps auf seinem Androiden installieren – doch das Einzige, was

damit garantiert ist, sind belegter Speicherplatz und Ressourcen-Verbrauch. Keiner der Hersteller wird garantieren, dass damit die Gefahr zu 100% gebannt ist, dass jeder Schädling erkannt und erfolgreich „abgeschossen“ wird.

Auf was sollte man also bei der Installation einer App achten?

Ist die Quelle vertrauenswürdig?

Positiv-Beispiele: AndroidPIT-Market, AppCenter, Google Playstore, Website des bekannten (!) Entwicklers

Negativ-Beispiele: Bei Rapidshare „gefunden“, in einer Tauschbörse aufgetrieben, per eDonkey aus unbekannter Quelle gezogen, ...

Sehen die Permissions vernünftig aus?

Positiv-Beispiele: Ein Webbrowser muss ins Web, eine SMS-App kann natürlich SMS lesen/schreiben/schicken und braucht ggf. auch (lesend) Zugriff aufs Adressbuch

Negativ-Beispiele: Eine Wallpaper-App braucht in der Regel keine Telefonnummern anzufragen, ein Ballerspiel muss keine SMS senden.

Besondere Vorsicht: Apps, die auf persönliche Daten (Kontakte, Kalender, Nachrichten) zugreifen und gleichzeitig ins Internet wollen. Leider lässt sich bei letzterem (Internet) die Frage der Notwendigkeit nicht so einfach beantworten – es könnte auch einfach nur für das Laden von Werbung nötig sein.

Was sagen andere Nutzer zur App/zum Entwickler (Bewertungen, Forum)?

Auch hier wieder GMV aktivieren. Kommentare wie „Geil!“, „Super“, etc. sagen nicht wirklich etwas aus (da hat eher jemand bei deaktiviertem GMV einen Kommentar hinterlassen).

Gleiches gilt für manchen negativen Kommentar: Nicht gerade selten passiert es, dass jemand einfach zu blöd war. Oder die Anforderungen der App gar nicht verstanden hat.

Nicht alle Bewertungen beziehen sich wirklich auf die App. Die kann schließlich nix dafür, wenn der Playstore mal wieder klemmt, und daher der Download nicht funktioniert. Oder die HD-Video-App, die mindestens WVGA benötigt, mit dem Motorola Flipout (mini-Display) im Playstore nicht gefunden wird, ...

Ganz neue App? Noch keine Bewertungen? Im Zweifelsfall im Forum nachfragen, ob schon jemand die App kennt und etwas dazu sagen kann.

Wer diese Punkte beachtet, hat eigentlich bereits mehr als die „halbe Miete“ eingefahren. Dann noch Vorsicht mit diversen Werbebannern, die einen mit Abos „beglücken“ wollen – und ein 90%iger Schutz sollte gegeben sein. Natürlich können andere Apps aus der „Sicherheits-Abteilung“ eine gute Ergänzung zu GMV bieten. Insbesondere bei Verlust des Gerätes – denn dagegen macht auch GMV nicht immun...

Rundum-Sorglos-Pakete

Die sollen einen wohl in Sicherheit wiegen – versprechen sie doch, sich um alles zu kümmern: Viren, Malware und Diebe sollen gleichermaßen eins auf die Mütze bekommen. Interessant ist hier: Nach einem Blick auf die verlangten Permissions müssten viele dieser Apps eigentlich gleich selbst draußen bleiben. Wozu bitte muss **Lookout Security Antivirus** (Bild 1.50) denn bitte Synchronisierungseinstellungen lesen/schreiben, Kontaktdaten lesen/schreiben, Kalenderdaten schreiben, Benutzerwörterbuch lesen/schreiben... Das Ding soll sich doch um die Abwehr der „bösen Jungs“ kümmern und nicht selbst an diesen persönlichen Dingen herumbasteln! Das kommt mir vor, als wolle man den Teufel mit dem Beelzebub austreiben.



Lookout Security
Antivirus



Bild 1.50: Lookout Security Antivirus verspricht Rundum-Schutz

Wer jetzt glaubt, die Antwort darauf in der App-Beschreibung zu finden: Fehlanzeige. Die Mühe, die ganze Website hinter dem angegebenen Link zu durchsuchen, habe ich mir nicht gemacht – zumindest in den dortigen FAQs findet sich auch keine Antwort. Ein Durchschnitt von 4,6 Sternen bei über 200.000 Bewertungen wirkt hingegen beruhigend: Offensichtlich wird mit den genannten Permissions wirklich nichts „Böses“ angestellt. Allerdings sollten sich die Entwickler solcher Software auf die Fahnen schreiben, hier mit gutem Beispiel voranzugehen, anstatt die Anwender zu verunsichern.

Davon abgesehen, klingt Lookout eigentlich recht vielversprechend: Jede heruntergeladene App wird hier auf „Schädlingsbefall“ geprüft. Zusätzlich kann man „Sicherheits-Kom-

plettskans“ seines Gerätes einrichten, die automatisch zum angegebenen Zeitpunkt (etwa wöchentlich) starten.

Das Gerät ist abhanden gekommen? Verlegt oder gestohlen? Per Google Maps lässt es sich lokalisieren (auch bei abgeschaltetem GPS; es wird dafür jedoch ein Account bei *myLook-out.com* benötigt). Auch ein lauter Alarm vom Gerät selbst kann ausgelöst werden – sogar wenn es gerade auf „lautlos“ steht. Als Dreingabe gibt es noch Backup und Restore wichtiger Daten, was Grund für einige der oben genannten Permissions sein dürfte. Das Schöne an der Sache: All dies ist gratis.



Kaspersky Mobile Security



Norton Mobile Security

Auch die Großen im Bereich Antivirus & Co. sind hier natürlich vertreten – wie etwa Kaspersky mit seiner **Kaspersky Mobile Security** (Bild 1.51) oder Symantec mit der **Norton Mobile Security**. Beide dürfen sich die gleichen Vorwürfe bezüglich der verlangten (und nicht begründeten) Permissions machen lassen. So möchte die Norton-Suite u. a. gern irgendwo anrufen, lesend und schreibend auf die Kontaktdaten zugreifen und so weiter. Bei Kaspersky sieht es nicht besser aus: Auf Kontaktdaten und Kalender möchte die App lesend und schreibend zugreifen (sicher für den Vermerk, wer das Gerät wann gestohlen hat). Anrufen möchte auch diese App irgendwo sowie an den Synchronisierungseinstellungen und APN-Einstellungen basteln. Bei einer solchen Kombination läuten eigentlich bei mir sämtliche Alarmglocken und schreien: Vorsicht, Malware!



Bild 1.51: Auch Kaspersky bietet ein „Rundum-Sorglos-Paket“ – verlangt dafür aber umfangreiche Berechtigungen

Was aber bringt Eugen Kaspersky uns nun mit seiner App bzw. was verspricht er uns als Gegenleistung für die gut sieben Euro? Echtzeit- sowie „On-Demand“-Scans nach Viren und Malware, Privacy für Kontakte (bestimmte Kontakte markieren, sodass keine Spuren der Kommunikation mit ihnen zu sehen sind – aha, das erklärt zumindest die Zugriffe auf die Kontaktliste), Anruf- und SMS-Filter, Diebstahl-Schutz (Lock, Wipe, Anzeige einer Nachricht wie z. B. „Ich wurde verloren/gestohlen, bitte xxx anrufen“, Anzeige der Location in Google Maps sowie E-Mail-Alert mit neuer Rufnummer bei SIM-Wechsel – sofern der Dieb nicht schlau genug war, vorher einen Wipe zu machen).

Genauer erkundigen sollte man sich auch noch, ob zu den gut sieben Euro für die App selbst noch jährliche Kosten von 25 Euro hinzukommen, wie verschiedentlich im Forum berichtet wurde.

NetQin Security & Anti-virus (Bild 1.52) gehört ebenfalls hierher – bietet es doch gratis nicht nur Schutz vor Viren und Malware, sondern, wie der Screenshot zeigt, auch einen Diebstahlschutz und sogar einen Traffic-Manager. Hinzu kommt auch noch ein System-Monitor mit Anzeige der Speicherauslastung und Taskkiller sowie „Geräte-Optimierung“ mit der tollen Ansage „Increase efficiency by closing apps that run in the background without your knowledge“. Ich hoffe, das ist lediglich als Vorschlag gemeint – und beschreibt nicht etwas, was die App ohne Rückfrage selbst tut. Ach ja: Ein Monitor für Zugriffe auf private Daten ist ebenfalls mit dabei, „böse Apps“ werden zur Deinstallation gezwungen („force uninstall“), und obendrein kann man auch die Kontakte sichern und wiederherstellen.



NetQin Security & Anti-virus

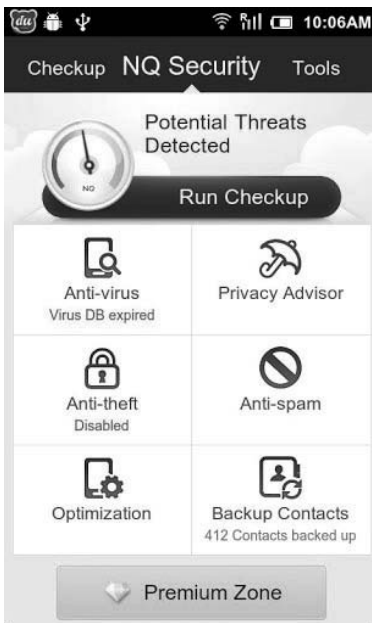


Bild 1.52: NetQuin möchte so ziemlich alles können – insbesondere aber alles dürfen...

Dem Umfang der App entsprechen auch die wieder einmal nicht begründeten Permissions. Wer alles können will, muss natürlich viel anfordern – doch bei einigen Dingen sollte man dennoch angeben, wozu sie genutzt werden. Da fordern Kaspersky & Co. in ihren Sicherheitsberichten doch explizit auf, man solle nichts installieren, was suspekte Permissions fordert – und dann liefern sie gleich selbst die Beispiele dafür? Wozu möchte beispielsweise *NetQin* Systemeinstellungen oder UI-Einstellungen ändern, Synchronisierungseinstellungen schreiben, Telefonnummern direkt anrufen sowie lesend und schreibend auf die Kontaktdaten zugreifen? Genau so stellt man sich die Permissions von Malware vor – hier täte eine genauere Beschreibung dringend Not!

Aber was verspricht *NetQin* denn nun zu leisten? Die Bereiche habe ich ja bereits grob umrissen: Die App kümmert sich um Viren, Malware und Diebstahl-Schutz. Ersteres sowohl in Echtzeit- als auch als „Device-Scan“. Für Letzteres ermöglicht es die Anzeige der gegenwärtigen Position des Gerätes auf der Karte, eine Sperrung des Gerätes, das Auslösen eines lauten Alarms, und auch das Löschen aller persönlichen Daten. Hinzu kommen noch Tools zum Sichern persönlicher Daten, Memory-Booster, Task-Killer, Traffic-Monitor, File-Manager ... Da stellt sich die Frage, was die App eigentlich nicht machen soll?

Anti-Virus und Anti-Malware



Dr.Web Anti-virus

Darum geht es in diesem Kapitel ja eigentlich: Malware, Viren und die dazugehörigen Gegenmittel. Mensch holt sich bei Virenbefall (oder vorbeugend) eine Impfung beim Doktor – und Androide greift beispielsweise zu *Dr.Web Anti-virus* (Bild 1.53). Endlich mal eine App, die auch bei den Permissions mit gutem Beispiel vorangeht! Zwar wird auch hier nicht erklärt, wozu die App z. B. die „Netzwerkonnektivität ändern“ muss – doch damit hat es sich auch bereits: Nur vergleichs-

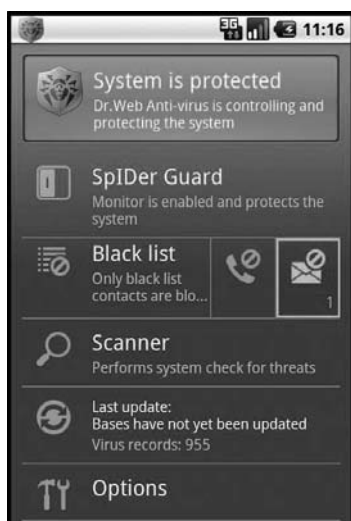


Bild 1.53: Dr. Web Anti-virus: Beliebt und sparsam in Bezug auf Berechtigungen

weise wenige Permissions werden angefordert, und diese sind (mit genannter Ausnahme) durchaus nachvollziehbar. Zudem sind App und Hersteller bereits aus dem PC-Bereich bekannt, und auch durchschnittliche 4,6 Sterne bei über 25.000 Bewertungen sind geeignet, Vertrauen zu erwecken.

Und was hat der Herr Doktor studiert, was kann er? Die Gratis-Version scannt einfach auf „böse Dateien“ und sperrt diese. Hierbei scheint sowohl ein Echtzeit-Scan zu erfolgen als auch die Möglichkeit zu einem „On-Demand-Scan“ zu bestehen. Außerdem lässt sich noch einstellen, dass auch die SD-Karte bei jedem Einbinden geprüft werden soll. Die Vollversion bietet dazu auch eine Filterung eingehender Anrufe und SMS, inklusive Blacklist (z. B. für nervige Werbe-Anrufer und Spam-SMS).

Hinter **Anti-Virus Free** (Bild 1.54) steht die auch vom PC-Anti-Viren-Markt her bekannte Firma AVG. Und bei der App beschränkt man sich schon längst nicht mehr auf das, was der Name suggeriert: Mit an Bord sind auch App-Locker, Task-Killer, Backup, Diebstahlschutz ... Kurzum: Auch AVG möchte einen Alleskönner präsentieren.

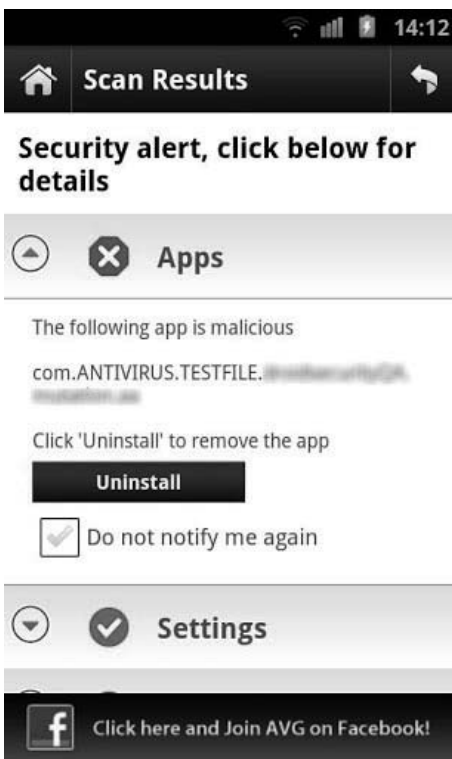


Bild 1.54: *Anti-Virus Free* von AVG bietet neben Malware-Schutz auch einige Zusatz-Funktionen

Was er definitiv kann, ist jede Menge Permissions anzufordern – ohne sie zu erklären. Offensichtlich eine verbreitete Unsitte bei allen Apps in diesem Segment (mit wenigen

Ausnahmen): Ich habe einen Namen, ich darf das. Auch hier darf sich der Anwender wieder vergeblich fragen: Wozu bitte will diese App Systemeinstellungen ändern, Synchronisierungseinstellungen schreiben, abonnierte Feeds schreiben, Kontaktdaten lesen und schreiben (da steckt vermutlich das Backup dahinter), das Benutzer-Wörterbuch schreiben (aber nicht lesen?), Kalenderdaten schreiben (aber nicht lesen – hier ist also kaum das Backup der Grund) ...

Nun gut: Der Name ist bekannt, die Firma auch. Die Anzahl der Bewertungen liegt im sechsstelligen Bereich, der Schnitt ist über vier Sternen angesiedelt – alles Dinge, die geeignet sind, die gerade aufgeworfenen Zweifel ein wenig zu zerstreuen. Schauen wir uns also einmal an, was die App kann:

Es wird ein Echtzeit-Scan angeboten, der auch SMS und MMS einschließt. Dazu kommt ein Backup von Kontakten, Anrufprotokollen, Lesezeichen, Text- oder Medianachrichten auf die SD-Karte, Handyortung (durch SMS ausgelöst) sowie „Alarmton“ (auch wenn auf lautlos gestellt), Task-Killer, App-Locker (installierte Anwendungen gegen unbefugte Benutzung sperren) sowie der komplette Wipe, hier als „lokaler Wipe“ beschrieben. Keine Erwähnung von Benachrichtigung bei SIM-Wechsel oder der Möglichkeit, den Wipe remote auszulösen – aber auch diese Funktionalität dürfte enthalten sein.

Besonders schnell will es sein, einfach und unkompliziert, besser zu handhaben als *Look-out*, AVG & Kollegen. Die Rede ist von **MyAntiVirus Pro** (Bild 1.55). *Full protection for your Android-Phone against Spyware, Virus, Malware, Trojans!* Jawoll! Ob es halten kann, was es verspricht?



MyAntiVirus Pro

Bild 1.55: Dass es auch ohne viele Permissions geht, zeigt **MyAntiVirus Pro**

Zuerst unser obligatorischer Blick auf die geforderten Permissions. Was? Kann nicht sein – sicherheitshalber direkt im Google Playstore nochmal schauen: Tatsache! Die App will ja fast gar nichts! Scheinbar nur ins Internet für die täglichen Signatur-Updates. Vorbildlich! Oder, anders ausgedrückt: Wenn diese App es “ganz ohne” kann, wozu brauchen dann die anderen so viel davon? Oder kann die App hier gar nichts, und ist nur eine Demo? Dann wären die gut sieben Euro allerdings eine üble Abzocke. Und nicht einmal 200kB “groß” ist der Download – die anderen bislang betrachteten Apps brachten locker das Zehnfache auf die “Waage”...

Was bekommt man nun geboten? Laut App-Beschreibung deutschen Support, einen schnellen Anti-Virus-Scan, tägliche Signatur-Updates, sehr geringen Ressourcenverbrauch. Und was meinen die Anwender? Über 300 von ihnen haben die App bewertet, dabei kamen durchschnittlich gut 4,2 Sterne heraus. Die Kommentare lesen sich überwiegend positiv.

Zusammengefasst ist *MyAntiVirus Pro* eine der wenigen Apps in diesem Bereich, die sich auf ihre eigentlichen Aufgaben konzentriert, somit handlich und leicht bedienbar bleibt und überdies sparsam im Umgang mit Permissions sowie Ressourcen ist. Schade, dass sich die „Großen“ daran kein Beispiel nehmen.

AirPush & Co.

Eigentlich sind das ja alles Werbe-Netzwerke, die da mit Push-Notifications arbeiten. Der bekannteste Vertreter in dieser Gruppe ist sicher ***AirPush***. Warum ich denn Werbung an dieser Stelle behandle? Ganz einfach: Es gibt Werbung (die als solche klar erkennbar zu sein hat) – und es gibt solche, die Huckepack auf einer anderen App mitfährt, sich dann aber getrennt davon und als solche nicht klar erkennbar an ganz anderer Stelle zeigt. Das typische Verhalten eines Trojaners – womit diese Art von Werbung aus meiner Sicht definitiv in die Kategorie „Malware“ fällt.



AirPush



Bild 1.56: *AirPush & Co* blenden Werbung u. a. im Statusbereich ein

Ein Blick auf Bild 1.56 zeigt die Perfidität: Ist das jetzt eine System-Meldung, die mir Tipps für bessere Einstellungen für optimalere Akku-Laufzeit geben will? Mitnichten! Über einen „Klick“ auf derartige Einträge hat sich schon mancher Ungewolltes eingehandelt. Das Gemeine daran: Es ist nicht ersichtlich, woher das kommt – etwa welche App dafür verantwortlich ist. Fein raus ist da, wer bereits *Jelly Bean* auf seinem Androiden hat: Ein mit dieser Android-Version (4.1) eingeführtes neues Feature erlaubt, durch langes Drücken auf eine Notification den „Übeltäter“ zu entlarven – und ihm das „Übeltun“ zu untersagen. Und was machen die anderen 95% der Android-Anwender?



AirPush Detector

TrustGo
Ad-Detector

Natürlich muss niemand in die Röhre gucken. Recht bald nach Auftauchen dieser „Schädlinge“ fand sich auch die erste Software, die sie aufspüren konnte. Recht früh mit dabei und nach wie vor auch in der Bewertung an der Spitze ist **AirPush Detector**.

Und obwohl sich der Begriff „AirPush“ als Bezeichnung dieser Art von unlauterer Werbung etabliert hat, gibt es noch weitere Netzwerke dieser Art – weshalb in Folge auch einige Apps auftauchten, die möglichst viele dieser Übeltäter aufspüren wollten. Ein Beispiel dafür ist der abgebildete **Ad-Detector** von TrustGo. Wie im Screenshot bereits erkennbar, spürt diese App nicht nur AirPush-Trojaner auf: *TrustGo Ad Detector scannt und schützt Ihr Mobiltelefon vor möglichen Verletzungen der Privatsphäre und die Identität Lecks durch Anzeigen von Anwendungen über die am häufigsten verwendeten Werbe-Netzwerke angezeigt.* (Aus der App-Beschreibung).

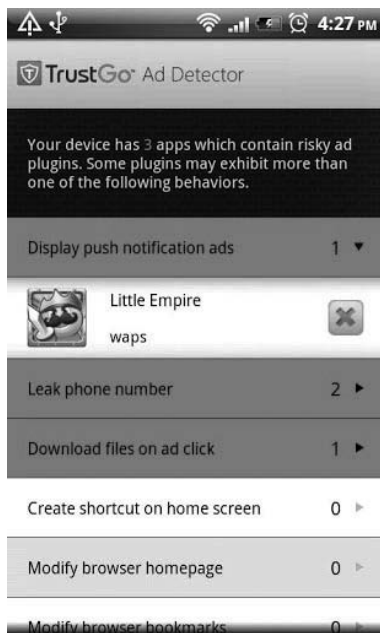
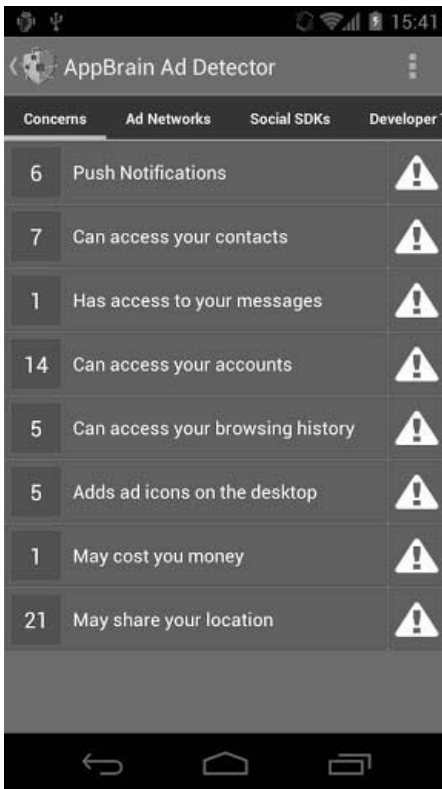


Bild 1.57: Der **Ad-Detector** von TrustGo steht ganz vorn auf der Beliebtheits-Skala, wenn es ums Aufspüren unliebsamer Werbe-Module geht

Damit man aber nicht erst warten muss, bis man sich bereits „infiziert“ hat, gibt es auch Vorsorge-Apps. So lässt sich etwa mit dem **AppBrain Ad-Detector** schon vor der Installation feststellen, welche App eventuell verseucht ist (Bild 1.58). Passenderweise wird das zusammen mit den verlangten Berechtigungen angezeigt. Wer ohnehin bereits auf die **AppBrain-Market**-App als gute und schnelle Alternative zur überladenen Playstore-App setzt, kann diesen Ad-Detector dort integrieren – so ist dann alles passend zusammengefasst: neue App gesucht, direkt geprüft, sofort entsorgt – und eine saubere Alternative gefunden sowie installiert ...



AppBrain
Ad-Detector

Bild 1.58: AppBrains **Ad-Detector** ermittelt die Bösewichter bereits vor der Installation der Apps

Lange genug hat dieser Ärger angehalten – doch endlich hat sich auch Google des Themas angenommen und die Regeln im Market verschärft. Diese Art von schlechter Werbung sollte es also in Zukunft schwerer haben. Warum ich das Thema dann hier dennoch so ausführlich behandelt habe? So mancher nutzt halt auch alternative Märkte. Und ob diese allesamt ebenfalls der Trojanischen Werbung den Kampf ansagen, ist weniger sicher.



<http://www.androidpit.de/google-entwickler-richtlinien-verbietet-airpush>



<http://www.androidpit.de/de/android/forum/thread/458671/>

Natürlich gibt es auch zu diesem Thema wieder eine passende *Übersicht bei AndroidPIT*, in der sich weitere Alternativen und Tipps finden. Wie beispielsweise der, zum Abschalten der Airpush-Werbung so ganz ohne App das *Opt-Out auf der AirPush-Website* zu nutzen – natürlich nur, wenn man auch betroffen ist.

Diebstahlschutz

Kann eine App wirklich vor Diebstahl schützen? Sicher nur bedingt. Dafür müsste sie den Dieb „in flagranti“ außer Gefecht setzen: Stromstoß, Tränen- und Nervengas, Keule auf die Rübe ... Menschenrechts-Kommission vor der Tür. Geht so nicht! Abgesehen von der schwierigen technischen Umsetzung.

Dass das doch zumindest ansatzweise geht, zeigt u. a. *Thief Alarm* (Bild 1.59): Hier soll der Dieb mit Sirenengeheul in die Flucht geschlagen werden. Der Krawall geht los, sobald man das Gerät bewegt, ohne rechtzeitig den Alarm-Code einzugeben. Eine Sache, die sich sicher auch mit *Tasker* (Abschnitt 2.5) umsetzen ließe – eventuell sogar mit einer Gesten-Deaktivierung (einmal kurz schütteln, einmal drehen: deaktiviert) ...



Thief Alarm

Bild 1.59: *Thief Alarm* will Diebe mit Sirenen-Geheul in die Flucht schlagen

Die meisten Anti-Theft-Apps sind eher die „Pille danach“ – sie greifen erst dann ein, wenn das Kind in den Brunnen gefallen und der Androide verschwunden ist. Die dann angebotenen Möglichkeiten fallen sehr unterschiedlich aus; vereinfacht ausgedrückt reichen sie von einfachen Lokalisierungshilfen bis hin zur Selbstzerstörungs-Automatik. Eindeutig in die erste Kategorie gehört das abgebildete **Wheres My Droid**: Ist der Droide verschwunden, benötigt man eben mal sein Zweitgerät, das Telefon eines Freundes oder einer beliebigen anderen Person. Damit schickt man sodann eine SMS mit dem „Attention Word“ (also dem passenden Code, den man zuvor konfiguriert hat) an das verschwundene Gerät – und es antwortet per SMS mit den Koordinaten. Ein Blick in Google Maps – aha, da isses (gerade)! Ein anderes „Attention Word“, und das Gerät macht mit ordentlich Krach auf sich aufmerksam. Auch wenn es gerade „ruhig gestellt“ (silent mode) war.

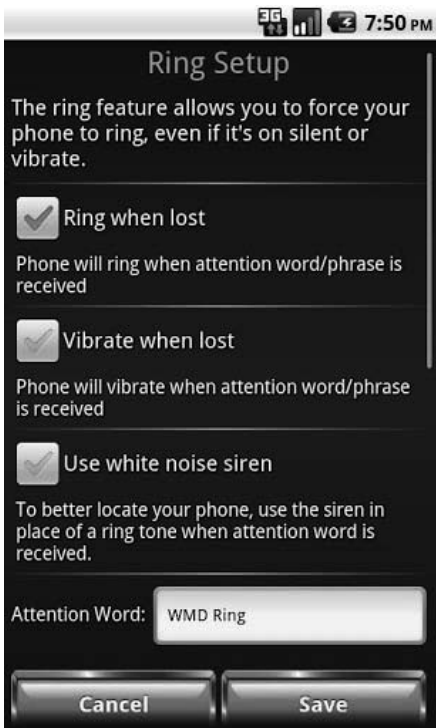


Bild 1.60: *Wheres My Droid* ermöglicht das Auffinden verschwundener Geräte, die mit dieser App ausgestattet sind

Das setzt natürlich voraus, dass die eigene SIM-Karte noch im Gerät steckt (sonst läuft die SMS ja ins Leere). Aber per E-Mail klappt es auch und sollte nach SIM-Wechsel auch noch funktionieren. Dabei benachrichtigt diese App allerdings nicht – auch ein „Wipe“ persönlicher Daten ist hier nicht vorgesehen.



Watch Droid

WatchDroid Lite kann dies auch, bietet aber zusätzlich einen „Stealth Mode“ (Tarn-Modus), damit der „Finder“ die App nicht einfach löscht. Krach zu schlagen und SMS mit GPS-Daten zu verschicken sollte damit kein Problem sein. **WatchDroid Pro** (Bild 1.61) bietet für etwa anderthalb Euro einen guten Mehrwert: Das Telefon lässt sich nun auch aus der Ferne sperren oder komplett löschen (Wipe). Auch ein eventueller SIM-Karten-Wechsel wird von der Pro-Version erkannt und mit dem Versand einer SMS an den hinterlegten Empfänger beantwortet. Der Trend geht eindeutig zum Zweitgerät ...



Bild 1.61: **WatchDroid** schützt sich mit einem Stealth-Modus gegen unbefugte De-Installation



GotYa! Face trap

Mehr als nur interessant klingt auch der Ansatz von **GotYa! Face trap** (Bild 1.62) – zumindest wenn der Androide über eine Front-Kamera verfügt. Bei jeder Falscheingabe des Entsperrcodes/Entsperrmusters schickt diese App ein Foto des „Täters“ inklusive eines Google-Maps-Links seiner gegenwärtigen Position per Mail. Per SMS lässt sich aus der Ferne auch jederzeit der gegenwärtige Standort abfragen, ein Rückruf auslösen oder ein Alarm abspielen (falls man das Gerät lediglich verlegt hat und es auf die letzten Meter „akustisch lokalisieren“ möchte). Die Vollversion benachrichtigt auch bei Wechsel der SIM-Karte.



Bild 1.62: *GotYa! Face trap* knippt den Dieb beim Entsperrversuch – sofern eine Front-Kamera zur Verfügung steht

Etwa zwei Euro kostet der Spaß, eine Gratis-Version zum Testen gibt es jedoch ebenfalls.

Dann wären da natürlich noch die als *Rundum-Sorglos-Pakete* aufgeführten Apps, die sich ja „mal so eben nebenbei“ auch noch mit um den Diebstahl-Schutz kümmern wollten. Und natürlich gibt es auch hier wieder eine Übersicht bei AndroidPIT, die noch eine ganze Reihe weiterer Apps zum Thema kennt.



<http://www.androidpit.de/de/android/forum/thread/425367/>

Wie beispielsweise das recht interessant klingende Tool **TotalCare – Remote Security**. Dies ermöglicht es (siehe Screenshot), noch die wichtigsten Daten vom verlorenen Gerät zu kopieren, bevor man ihm den Garaus in Form einer Löschung macht. Eine gute Sache, falls beispielsweise das letzte Backup schon ein wenig zurückliegt. Natürlich lässt sich auch der gegenwärtige Standort des Gerätes feststellen, ebenso erfolgt eine Benachrichtigung bei Wechsel der SIM-Karte.



TotalCare –
Remote Security



Bild 1.63: *Total Care* ermöglicht es, vor dem „Remote Wipe“ noch schnell die wichtigsten Daten in Sicherheit zu bringen

1.3 App-Sicherheit

Nachdem nun etliche Sicherheits-Apps besprochen wurden, wird es Zeit, das Wort einmal umzudrehen: Wie steht es um die App-Sicherheit? Denn was nützen all die tollen Sicherheits-Apps, wenn die Anwendungen selbst unsicher sind? Das beste Sicherheits-Schloss ist sinnlos, wenn man den Schlüssel auf dem Fensterbrett ablegt und dann auch noch das Fenster offen stehen lässt.

In diesem Kontext gilt es, mehrere Bereiche zu betrachten: Zum einen geht es um die auf dem Gerät gespeicherten Daten und zum anderen sind da die Daten, die über diverse Netzwerke übertragen werden. Werfen wir also einmal einen Blick auf beide Themen.

Gespeicherte Daten

Es soll ja vorkommen, dass jemand „zufällig“ ein Android-Gerät „findet“ (manchmal auch in der Tasche der Jacke, die der Eigentümer gerade trägt). Dieser „Finder“ kann nun lediglich daran interessiert sein, die „gefundene“ Hardware zu Geld zu machen – oder aber auch, die darauf befindlichen Daten zu nutzen. Besonders interessant sind dabei natürlich Benutzernamen und Passwörter, aber auch andere persönliche Daten – denn beide lassen

sich vorzüglich zum Identitäts-Diebstahl nutzen, um „im Namen des Eigentümers“ Einkäufe zu tätigen oder Spam zu versenden, um nur zwei Beispiele zu nennen. Daher sollten diese Daten – wenn überhaupt – auf sichere Weise auf dem Gerät gespeichert werden.

Wie so etwas sicher geschehen kann, dafür gibt es mehrere Ansätze, die zumeist etwas mit Verschlüsselungs-Techniken zu tun haben. Absolut klar sollte jedoch sein: Passwörter im Klartext (also ohne zusätzliche Hilfsmittel lesbar) auf dem Gerät zu speichern ist ein absolutes No-Go – selbst die Verwendung einer einfachen „Cäsar-Chiffre“ (siehe *Texte verschlüsseln* in Abschnitt 1.2) bietet da schon wesentlich höhere Sicherheit, auch wenn sie alles andere als sicher ist: Auch „Daten-Diebe“ sind von Natur aus faul; Klartext-Passworte sind ohne großen Aufwand nutzbar, für alles andere muss zunächst der Algorithmus ermittelt werden.

Wer jetzt meint, das wäre doch selbstverständlich, der lese bitte weiter. Denn offensichtlich ist dem nicht so. Zur Ermittlung einiger Schwachstellen habe ich ein Nandroid-Backup meines Motorola Milestone 2 genommen, welches ich gleich nach dem Rooten und der Installation eines Custom Recovery Images erstellt habe (Stock Android 2.2.2). Daraus habe ich die /data-Partition extrahiert und bin die Verzeichnisse durchgegangen. Da gibt es Erstaunliches zu entdecken ...

System-Daten

Beginnen wir bei „des Pudels Kern“: dem Android-System. Dies sollte ja gerade in diesem Punkt ein großes Vorbild sein – was auch weitgehend zutrifft. Finden sich hier etwa sensible Daten im Klartext? Leider ja.

Ein Beispiel, das ich hier aufführen möchte, ist die Datei /data/misc/wifi/wpa_supplicant.conf. Hier werden die konfigurierten WLAN-Accesspoints gespeichert. Ein Ausschnitt dieser Datei sieht etwa wie folgt aus:

```
network={
    ssid="platzhotel"
    psk="hotel123"
    key_mgmt=WPA-PSK
    priority=46
}
```

Da gibt es also einen WLAN-Accesspoint namens „platzhotel“, das WLAN ist mit WPA verschlüsselt. Der zugehörige Schlüssel lautet: „hotel123“. Bummer! Ja, tatsächlich: Alles im Klartext (Anmerkung: Die Daten habe ich natürlich leicht angepasst, um niemanden in Bedrängnis zu bringen). Hier lässt der Name des Netzes zudem noch leicht auf die Institution schließen: Es handelt sich offensichtlich um ein Hotel, welches den Namen „Platzhotel“ trägt. Ein deutscher Name, was die Location zusätzlich eingrenzt. Jetzt noch schnell die App **Location Cache** installiert und geschaut, wo der Eigentümer zuletzt unterwegs

war (WLANs werden hier ja separat ausgewiesen) – und mit etwas Glück findet man auch den passenden Platz.

Im Falle des WLANs eines Hotels oder Cafés ist dies vielleicht noch kein „großes Ding“, da die Betreiber ihren Gästen den Zugang meist auf simple Anfrage mitteilen. Die genannte Datei speichert aber auch die Zugangsdaten für sensiblere Firmen-Netzwerke, wenn genutzt – und spätestens hier wird so etwas zum Sicherheits-Risiko!

Daten von Hersteller-Apps

Hersteller und Netzbetreiber „segnen“ uns ja mit weiteren vorinstallierten Apps. Manche davon sind auch wirklich für die breite Masse nützlich – andere möchte der Anwender viel lieber loswerden (siehe **Bloatware** im Anhang *Begriffserklärungen*). In die erste Kategorie gehört u.a. auch eine App zum Empfang, Lesen und zum Versand von Mails – die sich möglichst mit vielen Anbietern verträgt.

Hierfür sorgt u. a. auch HTC bei seinen Geräten, und die App ist recht beliebt. Insbesondere auch bei denjenigen, die etwa auf ihre Firmen-Mails auf dem Exchange-Server zugreifen möchten. Und hier lauert er wieder, unser „schwerwiegender Systemfehler“ namens „Zugangsdaten im Klartext“: Account, Passwort und sogar Domain-Daten lassen sich so direkt einsehen! Wie das an einem Beispiel aussieht, beschreibt Andrew Hoog in seinem Buch „Android Forensik“:

Ein konkretes Beispiel, das bei den Sicherheitsbeauftragten von Firmen die Alarmglocken läuten lassen sollte, ist die Art, wie der Android-eigene Mail-Client bei Verwendung des Microsoft-Exchange-ActiveSync(EAS)-Protokolls die Zugangsdaten speichert. Bei diesen handelt es sich um Namen und Passwort des Domain-Users. Viele Firmen zentralisieren die Services von Authentifikation, Autorisierung und Accounting (AAA) mittels ActiveDirectory, um so »Single SignOn« und eine vereinfachte Verwaltung zu ermöglichen. Im Allgemeinen führt diese Vereinfachung zu einer effektiveren Sicherheit. Die Android-Mail-App (com.android.mail) speichert die Zugangsdaten jedoch im Klartext an einem fest definierten Ort: Die Datenbank befindet sich im Verzeichnis /data/data/com.android.email. Die Verzeichnisstruktur sieht dabei folgendermaßen aus:

```
ahoog@ubuntu:~$ tree com.android.email/
com.android.email/
├── cache
│   └── webViewCache
├── databases
│   ├── 1.db_att
│   │   ├── 1
│   │   ├── 2
│   │   └── 3
```

```

|   └─ EmailProviderBody.db
|   └─ EmailProvider.db
|   └─ webViewCache.db
|   └─ webView.db
└─ files
    └─ deviceName
└─ lib
    └─ shared_prefs
        └─ AndroidMail.Main.xml

```

Das Passwort befindet sich in der Datenbank EmailProvider.db in der Tabelle HostAuth, wobei die Spalte praktischerweise auch noch password heißt:

```

ahoog@ubuntu:~$ sqlite3 com.android.email/databases/EmailProvider.db
SQLite version 3.6.22
Enter „.help“ for instructions
Enter SQL statements terminated with a „;“
sqlite> .mode line
sqlite> select * from HostAuth;
    _id = 1
  protocol = eas
    address = owa.CorpExchangeServerExample.com
      port = 0
     flags = 5
    login = diesIstDerBenutzernameImKlartext
  password = diesIstDasPasswortImKlartext-Ernsthaft!
    domain = esKannNichtSchadenAuchDomainInfoZuHaben
accountKey = 0

```

Zusätzlich zu Benutzername, Passwort und Domain werden auch der Betreff sowie der gesamte Mail-Body im data-Verzeichnis gespeichert – einschließlich Dateianhängen, Einstellungen und weiterer Information. Das alles natürlich im Klartext (da fällt einem das Wort »Silbertablett« ein).

App-Daten

Wenn sich schon beim System solche Lücken finden, überrascht es sicher kaum, dass so etwas auch bei Apps auftritt. Ein wirklich extremes Beispiel liefert etwa die populäre App *Skype*, wie ein Artikel bei *AndroidPolice.com* ausführlich beschreibt.



<http://www.androidpolice.com/2011/04/14/exclusive-vulnerability-in-skype-for-android-is-exposing-your-name-phone-number-chat-logs-and-a-lot-more/>

Die App speichert nicht nur den Benutzernamen, Profildaten, Chat-Protokolle und mehr unverschlüsselt in diversen SQLite-Datenbanken in seinem Daten-Verzeichnis (unterhalb von `/data/data/com.skype.merlin_mecha/`), sondern sie hebt auch gleich noch sämtliche vom System vorgesehenen Sicherheitsmaßnahmen aus. Eigentlich haben nämlich nur die App selbst und natürlich *root* Zugriff auf diese Verzeichnisse. Skype legt dies jedoch anders fest und macht sie für „alle Welt“ lesbar und schreibbar! Beispiele aus dem verlinkten Artikel:

```
# ls -l /data/data/com.skype.merlin_mecha/files/shared.xml
-rw-rw-rw- app_152 app_152 56136 2011-04-13 00:07 shared.xml

# grep Default /data/data/com.skype.merlin_mecha/files/shared.xml
<Default>jcaseap</Default>
```

Damit lässt sich der Name des Anwenders ermitteln – und somit auch der Name des Verzeichnisses, in dem seine Daten gespeichert wurden. Aber auch ohne diesen Schritt wäre es zu finden gewesen: So viele Verzeichnisse gibt es hier nicht, und alles steht ja offen wie ein Scheunentor. Werfen wir also einen Blick auf die Daten dieses Benutzers:

```
# ls -l /data/data/com.skype.merlin_mecha/files/jcaseap
-rw-rw-rw- app_152 app_152 331776 2011-04-13 00:08 main.db
-rw-rw-rw- app_152 app_152 119528 2011-04-13 00:08 main.db-journal
-rw-rw-rw- app_152 app_152 40960 2011-04-11 14:05 keyval.db
-rw-rw-rw- app_152 app_152 3522 2011-04-12 23:39 config.xml
drwxrwxrwx app_152 app_152 2011-04-11 14:05 voicemail
-rw-rw-rw- app_152 app_152 0 2011-04-11 14:05 config.lck
-rw-rw-rw- app_152 app_152 61440 2011-04-13 00:08 bistats.db
drwxrwxrwx app_152 app_152 2011-04-12 21:49 chatsync
-rw-rw-rw- app_152 app_152 12824 2011-04-11 14:05 keyval.db-
journal
-rw-rw-rw- app_152 app_152 33344 2011-04-13 00:08 bistats.db-
journal
```

Hier gibt es also eine SQLite-Datenbank mit dem Namen `main.db`. Klingt verlockend. Und lässt sich mit einem beliebigen SQLite-Client öffnen – es darf ja jeder zugreifen, dank der tollen Zugriffsrechte. In dieser Datenbank findet sich u. a. eine Tabelle namens `ac-counts` – wenn das nicht interessant klingt! Und was da alles Schönes gespeichert ist: Kontostand, vollständiger Name, Geburtsdatum, Anschrift, Telefon, Mail-Adresse, Website, Biografie und mehr – kurzum alles, was man seinem Skype-Account anvertraut hat.

Übertragene Daten

Auch hier gilt wieder: Wer bei Problemen mit unverschlüsselt übertragenen Daten nur an Apps von „irgendwelchen kleinen Drittanbietern“ denkt: Fehlanzeige. Bis etwa Mitte 2011 taten sich hier insbesondere Facebook und sogar Google hervor, die zur Datenübertragung statt auf sicheres HTTPS auf unverschlüsseltes HTTP setzten – und zwar auch für Anmeldedaten. War das Gerät dann auch noch in einem offenen WLAN eingebucht, war es für potenzielle Angreifer ein Leichtes, diese Zugangsdaten abzugreifen – indem sie sich im selben WLAN anmeldeten und beispielsweise einen Sniffer einsetzten.

Zumindest haben die beiden Genannten diese Sicherheitslücke geschlossen. Heißt es nun also „generelles Aufatmen“? Keineswegs! Denn dieses Problem taucht leider immer wieder auf. Aktuellstes Beispiel ist die beliebte App **WhatsApp Messenger**, die bis vor Kurzem das Gleiche tat. Auch hier wurde die Lücke zum Glück bereits geschlossen. Doch wer weiß, wo sie sich als nächstes zeigt? Auch wenn die Beispiele deutlich machen, dass insbesondere Apps sozialer Netzwerke dabei gern in den Vordergrund geraten, zeigt das lediglich, dass es hier besonders auffällt, es bedeutet jedoch nicht, dass sich das Phänomen darauf beschränkt.

Auch diese Behauptung möchte ich nicht einfach so im Raum stehen lassen. So hat AndroidPIT-Mitglied Jörg Voß die Nachrichten-App **N24** genauer unter die Lupe genommen. Hatten deren Entwickler doch versprochen, nicht auf sensible Daten wie insbesondere die IMEI zuzugreifen – da diese den Benutzer eindeutig identifizierbar machen würde. Gewissermaßen wurde auch Wort gehalten. Doch stattdessen verwendet man nun die Geräte-ID, die ebenso eindeutig ist, und überträgt sie natürlich auch noch unverschlüsselt über das Netz. Als ob dies nicht ausreichen würde, ist Ziel der Übertragung auch noch ein Drittanbieter. Noch nicht schlimm genug? Es geht schlimmer: Bei diesem Drittanbieter handelt es sich um ein Werbe-Netzwerk (der Ziel-Server: *mobile.smartad-server.com* in Frankreich).



<http://www.androidpit.de/n24-kommt-zur-sache-nur-wie>

Aber wie kann man sich vor derartigen Problemen schützen? GMV allein hilft hier offensichtlich wenig: Man sieht so etwas einer App ja wohl kaum „von außen“ an. Und in den App-Beschreibungen wird sich kaum ein Satz finden wie „Wir übertragen ihre persönlichen Informationen zu Werbezwecken unverschlüsselt an Dritte“. Man könnte jetzt ständig sämtliche Blogs und News-Feeds verfolgen (mal ehrlich, wer macht so etwas – außer mir natürlich?), doch derartige Sicherheitslücken sind ja nicht bereits bei Erscheinen einer App bekannt.

Ein wichtiger Punkt dürfte definitiv deutlich geworden sein: Im Umgang mit offenen (und öffentlichen) Netzen besonders vorsichtig sein; erstere am Besten weitgehend meiden. Das schränkt das Risiko schon ein ganzes Stück ein.

Aber auch andere haben dieses Problem erkannt und bieten ihre Unterstützung an. So ist die Website des Services **appWatchdog** der Forensik-Firma *viaForensics* definitiv einen

Besuch wert. Hier nimmt man bekannte Apps genauestens unter die Lupe – und es ist nicht gerade leicht für eine App, die strengen Tests mit einem grünen Haken zu bestehen. Es ist eher erschreckend, wie viele Apps hier durchfallen: Schränkt man die Anzeige auf „Android“ und „Productivity“ ein, findet sich etwa kein einziger grüner Haken! Zwar sieht es für das iPhone nicht wesentlich besser aus (peinlicherweise ist der einzige grüne Haken hier bei „Google Mail“ gesetzt – da fragt man sich ernsthaft, warum die App das bei Android nicht geschafft hat?).

Das zeigt jedoch lediglich, dass es im Bereich mobiler Apps um die Sicherheit nicht sonderlich gut bestellt ist. Ein Blick auf die Details entschärft den Schreck häufig ein wenig, wie beispielsweise der Eintrag zu **K-9 Mail** zeigt: Keine unverschlüsselt gespeicherten Passwörter – jedoch werden Benutzernamen und Daten unverschlüsselt abgelegt.

Als einer der Köpfe hinter *appWatchdog* schreibt Andrew Hoog in seinem Buch „Android Forensik“ zu diesem Service:

Der appWatchdog-Service nutzt forensische und Sicherheits-Techniken, um zu ermitteln, ob Daten wie Benutzernamen, Passwörter, Kreditkarten-Nummern, u. a. unsicher gespeichert werden. Dieser Prozess schließt die Installation der App sowie ihre Ausführung auf anwenderspezifische Art ein. Anschließend wird ein forensisches Image des Gerätes erstellt und hinsichtlich persönlicher Informationen und Anwendungsdaten untersucht. Ergebnisse dieser Untersuchung werden zuerst dem Entwickler mitgeteilt und erst danach der Öffentlichkeit bekannt gemacht, um sie auch den Verbrauchern zur Verfügung zu stellen. Anwender können dann eine informierte Entscheidung darüber treffen, ob sie diese App weiter nutzen oder evtl. auf die Veröffentlichung einer sichereren Versionen durch den Entwickler warten wollen.

Jede App wird auf Grundlage diverser Kriterien untersucht, die auf ihrer speziellen Nutzung basieren. So würden beispielsweise bei einer App für mobiles Bezahlen insbesondere Benutzernamen, Passwörter, Anwendungsdaten und Kreditkarten-Nummern berücksichtigt. Bei anderen Apps wären hingegen Kreditkarten-Nummern eventuell irrelevant. Insgesamt werden die folgenden Kriterien detaillierter betrachtet, wobei die drei zuerst genannten sich auf die meisten Apps anwenden lassen:

- *Werden Passwörter sicher gespeichert? Sobald irgendeine Art von Passwörtern unverschlüsselt auf dem Gerät gespeichert wird, heißt das für die App: »Fail«.*
- *Werden Benutzernamen sicher gespeichert? Auch hier wird auf unverschlüsselte Speicherung geprüft.*
- *Werden Anwendungsdaten sicher gespeichert? Hier wird jede App hinsichtlich ihrer Anwendungsdaten untersucht. Bei Finanz-Apps beträfe dies u. a. Kontonummern, Kontostände und Transaktionsdaten. Bei anderen Apps könnten dies persönliche Informationen wie Email-Adressen, Telefonnummern oder Anschriften sein.*



<https://viaforensics.com/appwatchdog>

- Werden Kreditkarten-Informationen sicher gespeichert? Verwendet eine App Kreditkarten-Informationen, werden ihre Daten darauf untersucht, ob Kreditkarten-Nummern unverschlüsselt abgelegt werden – aber auch damit verknüpfte Informationen wie Ablaufdatum oder die auf ihrer Rückseite befindliche Sicherheits-Nummer.
- Zusätzliche Sicherheits-Tests: Diese können die Aufzeichnung drahtlos übertragener Daten und die Untersuchung derselben auf Benutzernamen, Passwörter, PINs und weitere relevante Anwendungsdaten umfassen. Diese zusätzlichen Sicherheits-Tests sind wesentlich aufwendiger und werden daher nur bei der vertieften Sicherheitsanalyse einer App durchgeführt.

Der appWatchdog-Service bietet grundlegende Hinweise darauf, ob eine mobile App Sicherheitstechniken implementiert.

Bei appWatchdog werden die Apps in Intervallen erneut geprüft – man sieht also, ob die Entwickler die Warnung ernst genommen haben. Erfreulich zu sehen, dass sich da bei einigen Apps tatsächlich etwas tut! Und übrigens: Wem eine App besonders am Herzen liegt, der kann auch ihre Prüfung auf der genannten Webseite anregen.

Weitere Sicherheits-Probleme

Als ob Obiges noch nicht genügt, bietet die Sicherheit noch einige andere Tücken – auf die ich hier nicht in voller Breite eingehen möchte. Ein paar Beispiele seien jedoch noch genannt:

Um die Authentizität von Apps zu gewährleisten, muss jede im Playstore eingestellte App mit einem Zertifikat signiert werden, welches den Entwickler eindeutig identifiziert. Dies erschwert es u. a. Betrügern, eine schädliche App als „Update“ einer beliebten anderen App auszugeben. Was aber, wenn ein solches Zertifikat einmal kompromittiert wurde, also „in fremde Hände“ geriet? Das mag zwar dem einen oder anderen Entwickler „peinlich“ sein – ein guter Zug ist es jedoch, die Anwender darauf unverzüglich hinzuweisen (etwa in der App-Beschreibung). Auf jeden Fall ist dann ein neues Zertifikat fällig.

Die Sache hat jedoch einen kleinen Haken: Neues Zertifikat heißt auch, dass Updates auf die mit dem alten Zertifikat signierten Versionen nicht mehr möglich sind (sonst wäre das System ja ad absurdum geführt). Besonders ärgerlich für die Anwender, die bei einem Update ihre Daten nicht mehr übernehmen können! Hier könnten Entwickler entsprechend Vorsorge treffen, indem sie – auch in den Gratis-Versionen ihrer Apps – einen Datenexport ermöglichen. Gibt es zu der App auch eine Kaufversion, könnten auf diese Weise auch dort die Daten dann übernommen werden. Ebenso wäre dies bei einer neuen Version mit neuem Zertifikat möglich.

Wer bis hierher mitgelesen hat, könnte nun denken: „Aha, wenn ich also auf Apps von Drittanbietern verzichte ...“ Leider nicht ganz. Zum einen haben obige Beispiele ja gezeigt,

dass durchaus auch vorinstallierte Apps betroffen sein können, und zum anderen macht Android so ganz ohne Apps ja auch nicht wirklich Spaß. Wer derart paranoid ist, sollte dann besser zu einem der „guten alten Knochen“ greifen, die lediglich Telefonie und SMS unterstützen.

Und dummerweise gibt es auch ohne Apps hin und wieder Sicherheitsprobleme – etwa mit proprietärer Software vom originalen Hersteller. So berichtet etwa Android-TV von einer Sicherheitslücke in der Software „Kies“, die Samsung für seine Geräte einsetzt (für die Daten-Synchronisation sowie auch für Firmware-Updates). Hier zeigte sich allerdings das vorbildliche Verhalten des Herstellers: Kaum war die Lücke bekannt, schon war sie wieder geschlossen. Und Hand aufs Herz: Vor Fehlern geft ist niemand – so etwas kann also wirklich jedem Entwickler passieren. Gut, wenn er dann so schnell reagiert wie in diesem Falle Samsung!

Wen das Thema noch näher interessiert, der findet im Netz natürlich weitere detaillierte Informationen, etwa in einem sehr ausführlichen Artikel der Computerwoche zum Thema **Android Sicherheitskonzept** oder in einem Blog bei AndroidPIT mit dem Titel **Android muss sicher werden**. Eine weitere empfehlenswerte Quelle ist das Buch *Android Forensics and mobile Security* von Andrew Hoog, das auch in einer deutschen Übersetzung („Android Forensik“, Franzis Verlag 2012) verfügbar ist.



<http://an-droid-tv.de/samsung-kies-sicherheitslücke-gefunden-und-schon-gestopft/>



<http://www.computerwoche.de/netzwerke/mobile-wireless/2497291/>



<http://www.androidpit.de/userblog-Offen-bedeutet-nicht-fuer-alle-zugaenglich-Android-muss-sicher-werden>

2 System

Im zweiten Teil dieses Buches soll es darum gehen, einen Überblick über das Android-System zu erhalten – und es in den Griff zu bekommen. Die folgenden Kapitel sollen daher Antworten auf die Frage „Wo finde ich was?“ liefern und aufzeigen, wie sich Dinge an den eigenen Bedarf anpassen lassen.

2.1 Der Super-User „root“

Von ihm ist in diesem Buch häufiger einmal die Rede, dem „Wurzel-Account“ (engl. „root“ = „Wurzel“), ohne den das Eine oder Andere einfach nicht funktioniert. Und da es sich dabei um den zentralen System-Account handelt, soll er in diesem Kapitel auch gleich als Erstes behandelt werden.

Für die Hersteller/Provider scheint es sich hier um „die Wurzel allen Übels“ zu handeln: Dieser Account hat so viel Power, dass man den Anwender da besser gar nicht erst heran lässt. Zu groß die Gefahren, dass er sich kurze Zeit später mit „Garantieansprüchen“ meldet, weil er „etwas kaputt gemacht“ hat. Die einzige mir bekannte Ausnahme betrifft den US-Provider *Cincinnati Bell*, der seine Kunden nicht länger auf ein Motorola-Update warten lassen wollte – und daher schlicht selbst eines erstellte. Damit die Kunden dies auch installieren konnten, wurde die Anleitung zum Rooten gleich mitgeliefert – bei voller Garantie durch den Provider selbst. Eine rühmliche Ausnahme, die aber noch immer nicht erklärt, um was es sich bei „root“ eigentlich handelt.

Kauft man einen Windows-PC, gibt es auf diesem einen Account für den Benutzer „Administrator“, dem man bei der Ersteinrichtung ein Passwort verpasst. Installiert man Linux, heißt das Pendant „root“. Android basiert auf Linux – aber trotzdem gönnen uns die Hersteller den root-Zugang in der Regel nicht, sondern drohen: „Wer sich root-Zugang zu seinem Gerät verschafft, verwirkt damit den Garantieanspruch.“

Damit ist nun klar, um was es bei dem Wort „root“ geht: Um den administrativen Zugang zum System, mit dem man alles (kaputt) machen kann. Na ja, fast alles – die Hardware wohl eher nicht. Weshalb die Warnung mit der Garantie wohl letztendlich vor Gericht kaum haltbar sein dürfte, wenn man z. B. das Display wechseln lassen muss, oder der interne Speicher den Geist aufgibt (anders sieht es aus, wenn die CPU verglüht, weil man sie hoffnungslos übertaktet hat – siehe Abschnitt *CPU übertakten* in Kapitel 4.5).

Braucht man den root-Zugang denn nun wirklich? Ja und nein. Wer mit seinem Gerät, dessen Funktionen sowie der verwendeten Software bereits rundum zufrieden ist, weil alles so läuft wie gewünscht, braucht auch keinen root-Zugang. Er hat ja bereits alles, was er braucht. Hat man hingegen ein Problem, das sich ohne den root-Zugang nicht lösen lässt, sieht das schon anders aus: Je nachdem, wie schwer es einen trifft, geht die Tendenz immer mehr zu „Mach mich root!“.

Um die Entscheidung zu erleichtern, schauen wir uns zuerst einmal die Vor- und Nachteile an, die mit dem Rooten verbunden sind:

Vorteile des root-Zugangs

Eine ganze Reihe von Apps setzt ein gerootetes Gerät voraus. Oder stellt auf einem solchen zusätzliche Funktionen bereit. Zahlreiche Einstellungen und Änderungen lassen sich ohne root-Zugang gar nicht vornehmen:

- **Übertakten** bzw. **Untertakten** der CPU – um entweder mehr Leistung herauszukitzeln oder den Akku zu längerem Durchhalten zu animieren
- **Entfernen/Einfrieren vorinstallierter Apps** – Da kommen oftmals Dinge mit, die kein Mensch braucht. Ab Android 4.0 (aka *Ice Cream Sandwich*) lassen sich unerwünschte Kandidaten auch ohne root zumindest „einfrieren“, also deaktivieren.
- **Bearbeiten der Start-Events** und somit verhindern, dass unerwünschte Apps automatisch gestartet werden. Zwar gibt es auch Apps, die versprechen, das ohne root zu erledigen – doch werden die betreffenden Apps lediglich nach dem Start wieder aus dem Speicher geschossen, worauf sich die jeweiligen Apps meist einfach wieder starten. Mit root kann man den Start selbst verhindern.
- **Neu-Kalibrieren des Akkus** – eigentlich eher dem Android-System die Akku-Daten neu beibringen, indem veraltete Akku-Statistiken gelöscht werden. Als Folge davon ist die Anzeige der verbleibenden Kapazität/Laufzeit wieder genauer.
- **Optimierung der Speicherverwaltung** – personalisierte Einstellungen statt 08/15, damit der Droid wieder flüssiger läuft
- **Anlegen einer Swap-Datei** und somit Nutzung von „virtuellem RAM“
- **App2SD auch mit Android < 2.2**, bzw. die Nutzung erweiterter Varianten wie App2SD+/Link2SD
- Aufspielen alternativer Firmware (aka „**Custom-ROM**“)
- Ändern der Systemschriftart(en)
- Erstellen eines wirklich **vollständigen Backups** des Android-Systems (siehe auch im Anhang *Begriffserklärungen* unter **Nandroid Backup**)
- Einrichten einer **Firewall**
- Einfaches Erstellen von Screenshots, ohne viele Verrenkungen (auf Samsung GalaxyS geht das von Haus aus – und Android 4.0 bringt das auf alle Geräte)

Diese Liste ist keinesfalls vollständig (natürlich auch nicht nach Relevanz sortiert – die wäre ohnehin wieder sehr subjektiv). Mit root hat man quasi überall Zugang – keine Ecke des Android-Systems bleibt verschlossen. Genau da liegt auch das Risiko, aber da liegt es auch beim root-Zugang auf dem Linux-PC oder dem Administrator-Zugang beim Windows-PC.

Risiken des root-Zugangs

Die Risiken sind schnell mit einem Satz beschrieben: Falsch angewendet, kann man sich mit root-Zugang das System unbrauchbar machen. Im schlimmsten Fall verwandelt man gar seinen Androiden in einen Ziegelstein – wenn man z. B. ohne Sinn und Verstand die CPU hoffnungslos übertaktet, und diese schließlich den Hitzetod stirbt. Mit Wissen und Verstand eingesetzt, ist der root-Zugang ein mächtiges und nützliches Werkzeug. Quasi wie ein Autoschlüssel: Setzt sich der achtjährige Steppke hinters Steuer ... Damit ist wieder bewiesen, dass man uns für absolut unmündig hält oder sich schlicht vor unnötigen Rückgaben und Garantie-Einforderungen von zu ambitionierten Anwendern schützen will. Ein nachvollziehbarer Grund – denn solche Anwender gibt es leider zu viele.

Wie bekomme ich root-Zugang?

Das jetzt so zu erklären, dass es für jeden gilt, führt ein wenig zu weit. Für diese Übersicht kurz zusammengefasst, gibt es da mehrere Möglichkeiten – und je nachdem, um welches Gerät es geht, greift davon eine, keine oder mehrere.

Da ist zum einen „Software-root“: Man lädt sich die passende App auf den Androiden, startet sie und bestätigt: „Ja, ich will root!“. Fertig. Toll: Mit so einem Gerät fühle ich mich absolut sicher. Wer sagt mir, dass eine andere App das nicht im Hintergrund tut, ohne mich zu fragen? Die meisten dieser Apps haben allerdings mit *Gingerbread* ohnehin ihren Dienst eingestellt.

OK, auch die zweite Variante ist im Prinzip eine Art „Software-root“ (schließlich geht es ja um Software-seitigen Zugang). Nur geht es hier nicht um eine „einfache App“, sondern es ist schwieriger: Zunächst muss das USB-Debugging im Gerät aktiviert werden (expliziter Schritt, schwer von einer App auszuführen). Dann ist der Androide per USB-Kabel mit dem PC zu verbinden (unmöglich, dass das eine App im Hintergrund macht). Und schließlich muss man auf dem PC die „root-Software“ starten, die über das Kabel auf das Android-Gerät zugreift. Die Schritte sind noch immer einfach und nachvollziehbar – aber hier habe ich keine Bedenken, dass das ohne mein Zutun passieren könnte. Leider sind die meisten „Allrounder“ aus dieser Kategorie (wie etwa das bekannte SuperOneClick) auf ein auf dem PC laufendes Windows angewiesen – womit Mac-OS- und Linux-Anwender im Regen stehen bleiben.

Welche Variante für ein bestimmtes Gerät verfügbar ist und welche Software dafür benötigt wird, recherchiert man am besten im Internet. Bei AndroidPIT gibt es gerätespezifische Foren (z. B. eines für das HTC Wildfire, eines für das HTC Desire, für das Motorola Milestone und so weiter). Jedes dieser Foren hat ein Unter-Forum für root-Fragen – dort finden sich die Informationen, die für das jeweilige Gerät zutreffend sind. Auch ein Blick in den root-Artikel des AndroidPIT-Wikis kann sich für weitere Informationen als nützlich erweisen.



[http://www.
androidpit.de/
de/android/wiki/
view/Root](http://www.androidpit.de/de/android/wiki/view/Root)

Laufen dann alle Apps mit root-Rechten?

Eine oft aufkommende Befürchtung – zum Glück unbegründet. Also die kurze Antwort: Nein, nicht ohne ausdrücklichen Wunsch des Anwenders.

Für eine detaillierte Antwort muss ich etwas tiefer greifen. Und wir müssen uns in Erinnerung rufen: Ein Android-System läuft ja mit Linux, also gelten hier auch entsprechende Richtlinien. Und jede App läuft darüber hinaus unter einem eigenen Benutzer. Auch root ist ein Benutzer, wenn auch ein ganz spezieller. Und wenn eine „normale App“ etwas mit root-Rechten ausführen möchte, muss sie „root“ dazu auffordern. Der Befehl dazu heißt `sudo`, was wir in unserem speziellen Kontext mit „SuperUser, DO ...“ wiedergeben können.



Bild 2.1: SuperUser blendet standardmäßig eine Nachricht ein, wenn es einer App root-Rechte gewährt

Läuft sie jedoch nicht unter „root“ (und das ist bei Android die Regel; jede App läuft – wie bereits gesagt – unter einem eigenen User), dann muss sie für Aktionen, die root-Rechte benötigen, root halt höflich bitten. Und das tut sie, indem sie dem auszuführenden Befehl ein „sudo“ (unter Linux; bei Android heißt der Befehl dazu schlicht „su“) voranstellt. Also „sudo <Befehl>“. Derart geweckt, schaut der SuperUser in seiner „Datenbank“ nach, ob die App denn so etwas darf. Beim ersten Aufruf steht sie da noch nicht drin: Die Folge ist ein Popup der SuperUser-App „App xyz möchte etwas mit SuperUser-Rechten machen. Darf sie das?“. Dazu zwei Buttons für „Ja“ bzw. „Nein“ sowie eine „Checkbox“, ob sich SuperUser diese Entscheidung für die Zukunft merken soll.

Bei jedem weiteren Aufruf findet der SuperUser die App in seiner Datenbank mit dem Vermerk „die darf das immer“ und führt den Befehl direkt aus. Zur Sicherheit wird dieser Fakt jetzt nochmals als Hinweis eingeblendet (siehe vorigen Screenshot). Die App wird dabei nicht gebremst, es ist auch keine Interaktion nötig. Daher sollte das in diesem Falle dann sogar vom Lockscreen aus funktionieren. Etwas störend ist es natürlich im Falle einer Screenshot-App – wie das Bild zeigt –, da dieser Hinweis dann auf jedem Bild verewigt ist. Deshalb lässt er sich auch in den Einstellungen der SuperUser-App abschalten.

Gibt es irgendwo weitere Infos zu diesem Thema?

Wer noch unsicher ist, findet im Netz natürlich weitere Informationsquellen – überwiegend in Foren und Wikis. Eine kleine Auswahl sei hier kurz aufgeführt:

- AndroidPIT-Forum: **Wozu Rooten/Flashen?**



<http://www.androidpit.de/de/android/forum/thread/431026/>

- AndroidPIT-Blog: **Rooten leicht gemacht** (11/2011)



<http://www.androidpit.de/Android-rooten-leicht-gemacht-Das-Easy-Rooting-Toolkit>

- Brutzelstube: **Rooten – und Garantie?**

In der Brutzelstube gibt es noch zahlreiche weitere Informationen, insbesondere – aber nicht ausschließlich – zu Themen rund um root, z. B. auch diverse root-Guides



<http://www.brutzelstube.de/2011/garantie-gewahrleistung-rooten-und-custom-roms/>

- Wikipedia (EN): **Rooting (Android OS)**



http://en.wikipedia.org/wiki/Rooting_%28Android_OS%29

- Wikipedia (DE): **CyanogenMod** – einer der besten Gründe pro root



<http://de.wikipedia.org/wiki/CyanogenMod>

- DroidWiki (DE): **Root** (und weitere interessante Themen rund um Android)



<http://www.droidwiki.de/Root>

- App: **ROM Toolbox** – Werkzeugkasten für Wurzelmenschen (siehe Abbildung rechts), mit ROM-Manager, App-Manager, CPU-Manager, Font-Installer, Root-Browser (FileManager)...



ROM Toolbox



Bild 2.2: ROM Toolbox ist ein Werkzeugkasten für Wurzelmenschen

2.2 Dateisysteme und Datenstrukturen

Um zumindest ansatzweise die Grundlagen zum Verständnis einiger technischer Eigenheiten zu vermitteln, soll an dieser Stelle auf einige Spezifika des Android-Systems eingegangen werden.

Der Boot-Prozess

Streng genommen, gehört er nicht direkt zum Thema „Dateisysteme und Datenstrukturen“. Doch im Verlauf des Boot-Prozesses werden zumindest die Dateisysteme bereitgestellt. Im Gesamt-Zusammenhang ist das Verständnis des Boot-Prozesses auch für einige andere Themen interessant.

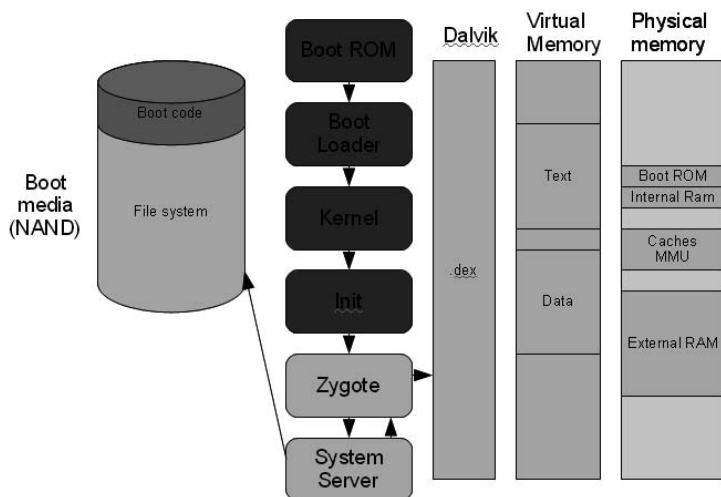
Einen guten Überblick gibt der Artikel *The Android boot process from power on*, der die einzelnen Schritte beschreibt und auch grafisch veranschaulicht.



<http://www.android-enea.com/2009/06/android-boot-process-from-power-on.html>

Detaillierter geht auch Andrew Hoog in seinem Buch „Android Forensik“ auf dieses Thema ein, wobei auch er auf den genannten Artikel als Grundlage zurückgreift. Zusammengefasst, lassen sich die sieben Schritte wie folgt beschreiben:

- Einschalten des Gerätes und Ausführung des Boot-ROM-Codes
- Bootloader
- Linux-Kernel
- Init-Prozess
- Zygote und Dalvik
- System-Server
- Boot Completed



Der Android-Boot-Prozess

(Quelle: <http://www.androidenea.com/2009/06/android-boot-process-from-power-on.html>)

Einschalten des Gerätes und Ausführung des Boot-ROM-Codes

Direkt nach dem Einschalten eines Android-Gerätes wird ein spezieller, mit der CPU verbundener Boot-ROM-Code ausgeführt, der die Geräte-Hardware initialisiert und das Boot-Medium lokalisiert. Dieser ROM-Code ist speziell an die vom Gerät genutzte CPU angepasst. Dieser Schritt im Boot-Prozess lässt sich grob mit dem von Computern genutzten BIOS vergleichen.

Wurde die Gerätehardware initialisiert, sucht der ROM-Code nach dem Bootmedium (welches bei Android-Geräten im NAND-Flash gespeichert ist) und kopiert den initialen Boot-Loader ins RAM. Anschließend springt die Ausführung aus dem Boot-ROM zum frisch in das RAM geladenen Code.

Bootloader

Der vom Bootmedium kopierte Boot-Loader wird nun im internen RAM ausgeführt. Dieser Schritt ist vergleichbar mit dem Starten des Boot-Loaders von Computern, etwa mit Windows, Mac OS oder Linux. Ein typischer Computer-Boot-Loader wie etwa GRUB für Linux erlaubt dem Anwender die Auswahl des gewünschten Betriebssystems und lädt es dann entsprechend.

Unter Android kümmert sich hier zunächst der Initial Program Loader (IPL) um die Erkennung und Einrichtung des externen RAM, kopiert den SPL dorthin und überträgt ihm die weitere Ausführung. Der Second Program Loader (SPL) lokalisiert sodann den Linux-Kernel und bootet das Medium, kopiert es ins RAM, lädt die Boot-Parameter und übergibt die weitere Ausführung schließlich an den Kernel.

Linux-Kernel

Nun übernimmt der Linux-Kernel die Kontrolle über das Gerät. Nachdem weitere Funktionalitäten des Gerätes eingerichtet wurden, wird das root-Dateisystem aus dem NAND-Flash gelesen, welches Zugriff auf das System und die Anwenderdaten bietet.

Init-Prozess

Sobald der Kernel Zugriff auf die Systempartition hat, kann er die Init-Skripte verarbeiten, die Schlüsselprozesse des Systems und der Anwendersoftware starten. Dies lässt sich mit den auf traditionellen Linux-Systemen verwendeten `/etc/init.d`-Skripten vergleichen. Unter Android findet sich das `init.rc`-Skript üblicherweise im Root-Dateisystem und vermittelt dem Kernel die Details für den Start der Kerndienste.

Zygote und Dalvik

Eine Eigenheit von Android ist es, dass es jede App in einer individuellen VM ausführt, die auch als »Sandkasten« bezeichnet wird. Die Dalvik-VM ist die von Google gewählte Technologie, diese Sandkästen zu erstellen. Beim Systemstart kümmert sich die Zygote-Sequenz hauptsächlich um die Konfiguration der Java-Laufzeitumgebung, und registriert ein Socket mit dem System – sodass neu gestartete Apps eine neue Dalvik-VM anfordern können.

System-Server

Sobald die Java-Laufzeitumgebung konfiguriert ist und der Zygote-Prozess bereitsteht, wird der System-Server gestartet. Dieser kümmert sich um Kernfunktionalitäten wie Telefonie, Netzwerk und weitere grundlegende Komponenten, auf die das Gerät und andere Apps angewiesen sind.

Steht alles bereit, sendet das System schließlich einen `ACTION_BOOT_COMPLETED` genannten Standard-Broadcast, welcher abhängige Prozesse davon in Kenntnis setzt, dass der Startvorgang abgeschlossen ist. Das Android-System ist nun voll funktionsfähig und bereit, mit dem Anwender zu interagieren.

Dateisysteme

Unter Android kommen verschiedene Dateisysteme zum Einsatz, die alle ihre Eigenheiten haben. Warum man sich nicht einfach auf ein Dateisystem festgelegt und dieses dann durchgängig verwendet hat? Würde das nicht Vieles vereinfachen? Vielleicht. Aber von unseren Hosentaschen-Computern erwarten wir schließlich, dass sie sowohl performant laufen als auch, dass der Akku möglichst lange durchhält. Zwei Dinge, die sich nicht gleichzeitig maximieren lassen – wie auch das Kapitel 4 *Tuning* noch zeigen wird. Jedes einzelne Dateisystem hat seine Vor- und Nachteile: Was für das eine Einsatzgebiet gut geeignet ist, passt nicht unbedingt auch für alle anderen.

Verfügbare Dateisysteme

Welche Dateisysteme finden sich nun auf dem Android-Gerät? Kommt ganz darauf an. Denn das unterscheidet sich wieder einmal von Gerät zu Gerät, Android-Version zu Android-Version, hängt ab von Hersteller, ROM-Küche und weiteren Eigenheiten. Doch jedes Android-Gerät verwendet mehrere (nicht jedoch unbedingt alle) der folgenden Dateisysteme:

- **EXT**

Das Extended Filesystem wurde 1992 speziell für Linux entworfen und seitdem ständig weiterentwickelt. Im Einsatz sind heute noch die Versionen 2–4 (ext2, ext3, ext4), die allesamt auch unter Android anzutreffen sind. Mit Version 3 wurde das Journal

eingeführt (womit das System sicherer und die Überprüfung schneller wird). Ext4 legte dann in Sachen Performance noch einmal zu.

- **procfs**
Bei procfs handelt es sich um ein virtuelles Dateisystem, das zur Ausgabe und Änderung von System- und Prozessinformationen dient (daher auch der Name: vom englischen *process*).
- **tmpfs**
Der Name lässt es bereits vermuten: Bei tmpfs handelt es sich um ein temporäres Dateisystem. Zum Einsatz kommt es auf RAM-Disks – also im Arbeitsspeicher – für Daten, die einen Reboot nicht überleben müssen/sollen.
- **reiserfs**
Das Reiser File System ist unter Android eher selten zu finden (obwohl es von einigen Custom-ROMs eingesetzt wird). Es war das erste Journaling-Dateisystem, welches vom Linux-Kernel direkt unterstützt wurde. Im Alltag trifft man überwiegend nur noch die neueren Versionen 3 und 4 an.
- **vfat**
VFAT steht für Virtual File Allocation Table, und kann sowohl auf FAT16 als auch FAT32 aufsetzen. Unter Android wird es ziemlich ausschließlich für SD- und eMMC-Karten eingesetzt.
- **YAFFS2**
YAFFS ist wieder einmal eine Abkürzung aus dem englischsprachigen Bereich. Wie so viele dieser mit YA beginnende Akronyme (Linuxer kennen das bereits) haben wir es auch hier mit „einfach etwas anderem“ zu tun: Yet Another Flash File System. Es wurde speziell für den Einsatz mit NAND-Flash entwickelt – eben jenem Speichertyp, der in fast allen mobilen Geräten (also auch in unseren Androiden) verbaut ist. Daher kennt YAFFS die entsprechenden Eigenheiten und kann so für eine längere Lebensdauer sorgen. In allen halbwegs aktuellen Android-Geräten wird die zweite Version davon eingesetzt – also YAFFS2.

Welche der genannten Dateisysteme auf einem spezifischen Gerät tatsächlich zum Einsatz kommen, lässt sich über das oben genannte `procfs` herausfinden:

```
$ adb shell cat /proc/filesystems
nodev    sysfs
nodev    rootfs
nodev    bdev
nodev    proc
nodev    cgroup
nodev    tmpfs
```

```

nodev  binfmt_misc
nodev  sockfs
nodev  usbfs
nodev  pipefs
nodev  anon_inodefs
nodev  inotifyfs
nodev  devpts
      ext3
nodev  ramfs
      vfat
      msdos
nodev  ecryptfs
      yaffs
      yaffs2
nodev  cifs

```

So sieht es beispielsweise auf meinem Motorola Milestone 2 mit *CyanogenMod 7.2* aus. Von den 21 hier unterstützten Dateisystemen betreffen nur fünf ein physisches Gerät wie etwa NAND-Flash oder SD-Karte. Die übrigen Dateisysteme sind mit dem Attribut `nodev` versehen, was bedeutet, dass es sich hier um virtuelle Dateisysteme handelt, die nicht auf einen physischen Speicher geschrieben werden.

Außerdem werden auch nicht alle unterstützten Dateisysteme unbedingt verwendet. Den 21 unterstützten Dateisystemen stehen nämlich in meinem Fall 18 eingebundene gegenüber:

```

$ mount|wc -l
18

```

Unterschiedliche Dateisysteme verbleiben dann schließlich nur noch neun:

```

$ mount | awk '{print $5}' | sort -u
cgroup
devpts
ext3
proc
ramfs
rootfs
sysfs
tmpfs
vfat

```

rootfs, devpts, sysfs und cgroup

Diese vier fehlen in der obigen Übersicht. Es handelt sich hier nämlich um sogenannte „virtuelle Dateisysteme“.

Zunächst wäre da *rootfs*, wo der Kernel das root-Dateisystem (die oberste Ebene des Verzeichnis-Baums, durch einen / gekennzeichnet) bei Systemstart einbindet. Damit der Kernel den Boot-Prozess abschließen kann, benötigt er Zugriff auf Kernbibliotheken und Dateien – daher muss er das root-Dateisystem einbinden. Während der Kernel den Boot-Prozess abschließt, werden weitere Dateisysteme in Unterverzeichnissen eingebunden.

Das Dateisystem *devpts* wird auf einem Android-System zur Bereitstellung virtueller Terminal-Sessions eingesetzt – vergleichbar mit der Verbindung zu einem traditionellen Unix-System unter Verwendung von *telnet* oder *ssh*. Jedes Mal, wenn sich ein virtuelles Terminal verbindet, wird unter */dev/pts* ein neuer Knoten erstellt. Zur Erstellung meiner Shell-Ausgaben habe ich mich beispielsweise mittels *ssh* mit meinem Milestone verbunden, was sich wie folgt widerspiegelt:

```
$ ls -l /dev/pts
crw-rw-rw- 1 app_38      app_38      136,  0 Sep 22 22:23 0
```

Benutzer und Gruppe sind hier eine gewisse *app_38*, das entspricht in meinem Fall der App *DroidSSH*. An diesem Beispiel lässt sich auch gleich eine Komponente des zuvor beschriebenen „Sandbox-Prinzips“ erkennen: Die App hat eine eigene User-ID und eine Gruppen-ID erhalten.

Sysfs ist ein anderes Dateisystem, das Konfigurations- und Steuerdateien für das Gerät enthält. Auf meinem Milestone 2 existieren hier die folgenden Verzeichnisse auf oberster Ebene:

```
$ ls -l /sys
drwxr-xr-x  2 root      root      0 Sep 22 22:32 block
drwxr-xr-x  2 root      root      0 Sep 22 22:32 board_
properties
drwxr-xr-x 12 root      root      0 Sep 22 22:32 bus
drwxr-xr-x 44 root      root      0 Aug  8 20:05 class
drwxr-xr-x  4 root      root      0 Sep 22 22:32 dev
drwxr-xr-x  7 root      root      0 Aug  8 20:05 devices
drwxr-xr-x  2 root      root      0 Sep 22 22:32 firmware
drwxr-xr-x  3 root      root      0 Sep 22 22:32 fs
drwxr-xr-x  4 root      root      0 Sep 22 00:21 kernel
drwxr-xr-x 86 root      root      0 Sep 22 22:32 module
drwxr-xr-x  2 root      root      0 Aug  8 20:05 power
drwxr-xr-x  2 root      root      0 Sep 22 22:32 smodule
drwxr-xr-x  2 root      root      0 Sep 22 22:32 usb_bypass
```


Hier lässt sich natürlich allerhand über das Android-System in Erfahrung bringen. Vieles davon kann man bereits an den aufgeführten Verzeichnisnamen erraten: So finden sich unter `/sys/block` Informationen über blockorientierte Geräte, unter `/sys/bus` u. a. auch Informationen über USB-Geräte (`/sys/bus/usb`) und so weiter.

Das letzte virtuelle Dateisystem nennt sich *cgroups* und wird genutzt, Tasks im Linux-Dateisystem zu verfolgen und zu aggregieren. Auf dem Motorola Milestone 2 wurden zwei *cgroups*-Dateisysteme erstellt: eins unter `/dev/cpuctl` und ein weiteres unter `/acct`.

proc

Das *proc*-Dateisystem bietet auf strukturierte Weise detaillierte Informationen über Kernel, Prozesse sowie Konfigurationsparameter, die im Verzeichnis `/proc` abgelegt sind. Einige dieser Dateien können vom Shell-User untersucht werden – doch viele verweigern den Zugriff, sofern man nicht über root-Rechte verfügt. Auf meinem Milestone 2 enthielt dieses Verzeichnis ca. 200 Einträge, weshalb ich mir ein vollständiges Listing an dieser Stelle spare.

Zunächst gibt es hier für jeden laufenden Prozess ein Unterverzeichnis mit Details zu selbigem, welches die Prozess-ID (PID) als Namen erhält. Da sich letztere recht einfach mit dem Befehl `ps` ermitteln lässt, können wir hier leicht einmal einen Blick hinter die Fassaden von *DroidSSH* werfen – das ja, wie erwähnt, bei mir gerade läuft:

```
$ ps |grep ssh
app_38      24885 3305  134344 25120 ffffffff afd0c82c S tk.tanguy.
droidsshd

$ ls /proc/24885
auxv          cmdline          environ          fdinfo          mem
<snip>

$ cat /proc/24885/status
Name:   anguy.droidsshd
State:  S (sleeping)
Tgid:   24885
Pid:    24885
PPid:   3305
TracerPid: 0
Uid:    10038 10038 10038 10038
Gid:    10038 10038 10038 10038
FDSize: 256
Groups: 1015 3003
```

```

VmPeak:   138488 kB
VmSize:   131128 kB
<snip>

```

Aber auch weitere Systeminformationen lassen sich hier untersuchen. Wie sieht es beispielsweise mit dem Arbeitsspeicher meines Droiden aus?

```

$ cat /proc/meminfo
MemTotal:      487344 kB
MemFree:       23028 kB
Buffers:       5076 kB
Cached:        85204 kB
SwapCached:    0 kB
Active:        166108 kB
Inactive:      201312 kB
<snip>

```

Und was für eine CPU steckt drin?

```

$ cat /proc/cpuinfo
Processor      : ARMv7 Processor rev 2 (v7l)
BogoMIPS      : 299.95
Features      : swp half thumb fastmult vfp edsp neon vfpv3
CPU implementer : 0x41
CPU architecture: 7
CPU variant    : 0x3
CPU part       : 0xc08
CPU revision   : 2

Hardware      : mapphone_UMTS
Revision      : 0000
Serial        : 0000000000000000

```

Dies nur als kurzen Einblick – hier alles aufzuführen würde den Rahmen dieses Buches sprengen. Wer mit Linux-Systemen vertraut ist, dem kam dies vermutlich ohnehin bekannt vor – und derjenige weiß auch, wo es weiter zu suchen gilt. Doch selbst ohne diese Vorkenntnis lässt sich vieles intuitiv finden.

tmpfs

Das *tmpfs*-Dateisystem speichert seine Daten in einem virtuellen Speicher, der im RAM und, sofern verfügbar, Swap- oder Cache-Bereich des Gerätes liegt. Die meisten heutigen Android-Geräte verfügen nicht über eine Auslagerungsdatei (Swap), doch einige Custom-ROMs aktivieren dieses Feature. Der Vorteil von *tmpfs* ist die Nutzung des RAMs: Es handelt sich damit um einen schnellen, nicht-permanenten Speicher, der bei einem Reboot nicht gesichert wird.

Schauen wir doch einmal, welche *tmpfs*-Dateisysteme auf meinem Milestone 2 eingebunden sind:

```
$ mount | grep tmpfs
tmpfs on /dev type tmpfs (rw,relatime,size=128k,mode=755)
tmpfs on /dev type tmpfs (rw,relatime,mode=755)
tmpfs on /mnt/asec type tmpfs (rw,relatime,mode=755,gid=1000)
tmpfs on /mnt/obb type tmpfs (rw,relatime,mode=755,gid=1000)
tmpfs on /mnt/sdcard/.android_secure type tmpfs
(ro,relatime,size=0k,mode=000)
```

Zwei interessante Kandidaten sind hier */mnt/asec* und */mnt/sdcard/.android_secure*: Diese werden nämlich von *App2SD* genutzt. Da auf die SD-Karte verschobene Apps dort verschlüsselt abgelegt werden (was als Kopierschutz gedacht ist), das System sie jedoch zur Ausführung entschlüsseln muss, kommt *tmpfs* zum Einsatz. Somit sind die entschlüsselten Daten beim Herunterfahren des Systems auch automatisch wieder verschwunden.

Das */dev*-Verzeichnis enthält die Gerätedateien, die dem Kernel das Lesen und Schreiben auf angeschlossenen Geräten wie NAND-Flash, SD-Karte, zeichenorientierten Geräten und anderen erlauben.

Extended File System (EXT)

Das speziell für Linux entwickelte EXT-Dateisystem hat, seit die erste Version 1992 das Licht der Welt erblickte, bereits drei Folgeversionen gesehen: EXT2, EXT3 und EXT4. Dennoch war es auf den ersten Android-Geräten nicht zu finden. Doch es gibt eine Reihe von Vorteilen, die dieses System auch für Androiden immer gebräuchlicher macht:

- EXT4 ist ein Linux-Dateisystem-Standard, der Unix-Permissions und Semantiken vollständig unterstützt.
- EXT4 ist stabil und bietet hohe Performanz.
- Das bislang hauptsächlich eingesetzte YAFFS ist single-threaded, was zu Engpässen bei Mehrkern-Prozessoren führen dürfte.
- Viele Android-Geräte wechseln von direktem NAND-Flash zu regulären Block-Geräten (eMMC).

FAT32/VFAT

Android-Geräte verfügen meist über eine oder mehrere mit Microsofts FAT32 formatierte Partition(en). Im Allgemeinen sind dies die SD-Karte und, sofern vorhanden, eMMC. Der Grund für die Wahl dieses Dateisystems ist nicht etwa die überlegene Technologie, sondern vielmehr die größtmögliche Kompatibilität mit anderen Betriebssystemen. Microsofts FAT32 wird von den meisten Betriebssystemen unterstützt, einschließlich Mac OS X, allen Windows-Versionen (offensichtlich), Linux und weiteren. Das bedeutet, dass von Android auf diesen Partitionen abgelegte Daten von anderen Betriebssystemen einfach gelesen, verändert oder gar gelöscht werden können.

Auf meinem Milestone 2 fand ich ganze zwei Partitionen, die VFAT nutzen: `/mnt/sdcard` (wie erwartet) und `/mnt/secure/asec`. Ersteres ist natürlich die SD-Karte, und letzteres begrüßt den Zugriffsversuch ohne root mit einem fröhlichen „Permission denied“. Der Name lässt bereits erahnen, dass es sich hier wohl um „Sicherheitsinformationen“ handelt, die mit *App2SD* in Verbindung stehen.

Bei `/mnt/secure/asec` handelt es sich um eine verschlüsselte Partition auf der SD-Karte, auf der Android-Geräte Apps speichern können. Als das Feature zur Installation von Apps auf der SD-Karte eingeführt wurde, befürchteten Sicherheitstechniker verständlicherweise, dass diese App-Daten auf einfache Weise beschädigt oder kompromittiert werden könnten – schließlich lassen sich auf VFAT/FAT32-Partitionen keine Zugriffsrechte verwalten. Daher wird die App (bzw. deren *.apk*-Datei) hier verschlüsselt abgelegt, zur Benutzung entschlüsselt und temporär unter `/mnt/asec` (oder einem anderen vom Design spezifizierten Verzeichnis) gespeichert.

YAFFS2

YAFFS2 wurde speziell für NAND-Flash-Geräte entwickelt und enthält eine Reihe wichtiger, die speziellen Bedürfnisse dieses Mediums betreffende Features. YAFFS2 ist:

- ein Log-strukturiertes Dateisystem (welches Daten selbst bei unerwartetem Stromausfall schützt)
- mit integriertem Wear-Levelling sowie Fehlerkorrektur (ECC) ausgestattet
- in der Lage, mit Bad-Blocks umzugehen
- schnell und hat nur einen geringen Bedarf an Arbeitsspeicher

YAFFS2 ist ein ausgeklügeltes, aber auch komplexes System. Es soll den Flash-Speicher möglichst schonen und begrenzt daher die Schreibzugriffe auf ein Minimum, um dessen Lebensdauer zu verlängern (NAND-Flash erlaubt nur eine begrenzte Anzahl von Schreibzyklen). Auf alle technischen Details einzugehen würde wieder ein wenig zu weit führen; interessierte Leser möchte ich daher auch in diesem Zusammenhang auf das Buch „Android Forensik“ von Andrew Hoog verweisen.

Datenstrukturen

Während wir uns zuvor dem Speicher eher von der Seite der dahinter stehenden Technologie und Fragen wie *Warum ist YAFFS2 so besonders gut für den Flash-Speicher geeignet?* genähert haben, geht es jetzt vielmehr um das „Wo“: Wo ist welches Medium eingebunden? Wo finde ich welche Daten?

Eingebundene Dateisysteme

Der „einfache Anwender“ weiß: Da ist Speicher drin und darauf liegen sicher die ganzen Dateien. Der Anwender mit ein wenig mehr technischem Hintergrund kann sich zumindest denken, dass der interne Speicher wohl auf einem anderen „Laufwerk“ liegt als die SD-Karte. Aber wer würde schon vermuten, dass es insgesamt 15 oder mehr sogenannte „Mount Points“ gibt – wobei sich hinter jedem ein eigenes Dateisystem verbirgt? Kein Witz, das ist tatsächlich der Fall! Einige davon seien hier kurz aufgeführt – wobei dies nur exemplarisch ist und nicht auf allen Geräten etc. übereinstimmen muss:

<i>Mount-Point</i>	<i>Typ</i>	<i>Kommentar</i>
/cache	ext3	Anwendungs-Cache
/data	ext3	Dalvik-Cache, Logs, Konfigurationsdateien ...
/data/data	YAFFS2	Anwendungsdaten
/dev	tmpfs	„Geräte-Dateien“ (devices)
/mnt/asec	tmpfs	„entschlüsselte“ Version der mit App2SD auf die Karte verschobenen .apk-Dateien
/mnt/emmc	vfat	interne „SD-Karte“ (eMMC)
/mnt/sdcard	vfat	externe SD-Karte
/proc	procfs	System- und Prozess-Informationen
/system	YAFFS2	vorinstallierte System-Dateien

Nicht bei allen Geräten/ROMs wird /data/data als separate Partition eingebunden – dann sind die hier abgelegten Daten natürlich auf der /data-Partition angesiedelt. Die in obiger Tabelle bezeichnete Partition bzw. das Verzeichnis /mnt/emmc ist auf vielen Geräten gar nicht vorhanden: Mein HTC Wildfire etwa verfügt nicht über diesen zusätzlichen Speicher. Und unter /mnt/sdcard kann natürlich auch nur dann etwas zu liegen kommen, wenn auch eine SD-Karte eingelegt ist (es soll ja Geräte geben, die diese Möglichkeit gar nicht bieten). Auf allen Android-Geräten sollten jedoch an genau diesen Stellen die standardisierten Mount-Points /data, /dev, /proc und /system vorhanden sein.

Dass `/dev` und `/proc` eine besondere Rolle spielen, ist zumindest eingefleischten Linux-Anwendern bekannt: An erster Stelle kann man nachschauen, welche „Geräte“ denn so erkannt wurden (so findet sich für die meisten anderen genannten Dateisysteme unter `/dev/block` das entsprechende „Block-Gerät“, über das auf den physischen Speicher zugegriffen werden kann). Und unter Letzterem lassen sich so einige System-Informationen auslesen (unter `/proc/mtd` etwa finden sich Informationen zu den im NAND-Flash angelegten Partitionen, und unter `/proc/sys/kernel` kann man verschiedene Kernel-Parameter auslesen oder auch anpassen). Doch auch `/system` hat eine Besonderheit: Es wird im reinen Lese-Zugriff eingebunden – Änderungen sind hier also nicht (ohne Weiteres bzw. ohne root-Rechte) möglich. In dieser Partition finden sich nämlich die System-Programme, aber auch all die tollen „Zwangs-Beglückungen“, die uns Geräte-Hersteller und ggf. Netzanbieter so gern „zur Verfügung stellen“.

Einen ganz speziellen Fall stellt auch das temporäre Dateisystem dar, das unter `/mnt/asec` eingebunden ist. Hat man nämlich mit *App2SD* Apps auf die SD-Karte ausgelagert, werden diese verschlüsselt im Verzeichnis `.android_secure/` gespeichert. In diesem verschlüsselten Zustand kann das System sie leider nicht ausführen. Daher werden sie zuvor entschlüsselt unter `/mnt/asec` abgelegt – von wo sie bei einem Systemstart automatisch wieder verschwinden.

Weitere Partitionen

Es gibt noch einige weitere Partitionen, von denen u. a. die folgenden noch interessant sein dürften:

Partition	Kommentar
<code>/boot</code>	Kernel & RAM-Disk
<code>/recovery</code>	Alternative Boot-Partition für Recovery Mode
<code>/sd-ext</code>	kein Standard; bei App2SD+ als „ausgelagerte <code>/data</code> Partition“ genutzt

Einige wichtige Verzeichnisse

An allem, was sich unterhalb von `/system` befindet, sollte nur wirklich „fachkundiges Personal“ arbeiten. Weitere interessante Verzeichnisse finden sich aber auch unterhalb von `/data`. Etliche davon werden für verschiedene Protokoll-Funktionen (auch als „Logging“ bekannt) genutzt; diese sind unter *Andere Logdateien* aufgeführt.

Unter `/data/data` befinden sich die von den Apps verwalteten Daten – wobei jeder App ein eigenes Verzeichnis zugewiesen ist, auf das (normalerweise) nur sie selbst Zugriff hat

(dass manch eine App diesen Schutz für die eigenen Daten aushebelt, wurde ja bereits zum Thema Sicherheit unter *App-Daten* gezeigt):

```
/data/data/com.example.demoapp
├─ cache                Verzeichnis
│  └─ webViewCache     Verzeichnis
│     └─ 027e59a0       Cache-Datei
│        └─ 057606c4    Cache-Datei
├─ databases
│  └─ example.db        SQLite-Datenbank
├─ lib                  Verzeichnis
└─ shared_prefs         Verzeichnis
   └─ example.xml       Konfigurations-Datei
```

So in etwa könnte das für eine „Beispiel-App“ aussehen – es können hier aber durchaus weitere Verzeichnisse vorhanden sein, oder nicht einmal alle aufgeführten. Unsere Beispiel-App hat also ...

- ein Cache-Verzeichnis und darin noch ein paar Dateien von Seiten, die aus dem Web geladen wurden
- ein Datenbank-Verzeichnis mit einer SQLite-Datenbank (es können natürlich auch mehrere sein), in der sie strukturiert Daten in mehreren Tabellen verwalten kann
- ein ominöses Bibliotheks-Verzeichnis ohne Inhalt
- ein Verzeichnis mit Konfigurations-Dateien im XML-Format

Die Zugriffs-Berechtigungen sollten hier normalerweise etwa wie folgt aussehen:

-rw-r----- für Dateien (der Eigentümer – also die App selbst – darf also lesen und schreiben, die Gruppe lesen und der Rest hat hier nichts zu suchen) sowie maximal drwxr-x--x für Verzeichnisse (Eigentümer darf lesen, schreiben und ausführen – für Verzeichnisse bedeutet das: Hineinwechseln – die Gruppe noch lesen und ausführen, der Rest allenfalls noch ausführen); wobei „der Rest“ hier eigentlich gar nichts mehr verloren hat.

Einige ausgewählte weitere Verzeichnisse (Quelle: mein Motorola Milestone 2, als es noch Stock-Firmware mit Android 2.2.2 hatte) möchte ich hier kurz aufführen:

```
/data
├─ backup                Google Backup Queue
│  └─ com.android.internal.backup.LocalTransport
│     └─ com.google.android.backup.BackupTransportService
│        └─ pending
```

├─ dalvik-cache	Dalvik-Cache
	(.dex (Dalvik EXecutable)-Dateien)
├─ local	Zwischenspeicher für zu
	installierende .apk-Dateien
├─ location	Der Location-Cache
	(„Ich weiß, wo Du...warst!“)
├─ misc	Verschiedene Konfigurations-Dateien
	├─ bluetooth
	├─ bluetoothd
	├─ dhcp
	├─ keystore
	├─ systemkeys
	├─ vpn
	└─ wifi
├─ preinstall_md5	MD5-Hash Dateien einiger
	vorinstallierter Apps
└─ system	Konfigurations- und Log-Dateien
├─ dropbox	Log-Dateien von Dropbox-Syncs
├─ registered_services	XML-Dateien mit Informationen zu
	verfügbaren (registrierten) Services
├─ security	Sicherheits-Zertifikate (binär)
├─ shared_prefs	Konfigurations-Daten (u. a. zu
	gesammelten Log-Dateien)
├─ sync	Einstellungen von
	„Kontakte & Synchronisation“:
	Welche Dienste sollen...?
└─ usagestats	Nutzungs-Statistiken

Eine Überraschung war für mich, dass das Verzeichnis `/data/system/dropbox` gut mit Protokollen (Zeitstempel für Beginn/Ende der Synchronisation) gefüllt war, obwohl ich nicht einmal ein Dropbox-Konto habe! In den `registered_services` war *Dropbox* auch nicht aufgeführt.

Im Verzeichnis `/data/system` finden sich überdies Dateien wie `accounts.db` (die Account-Datenbank mit konfigurierten Accounts, Authentifizierungs-Tokens und mehr), `appwidgets.xml` (Launcher und konfigurierte Widgets), `batterystats.bin` (Akku-Statistiken), `packages.list` / `packages.xml` (installierte Apps / App Permissions) und weitere.

Externer Speicher

Auf der SD-Karte sieht es auch immer recht wild aus – und so manch einer mag sich nicht nur einmal gefragt haben, ob hinter dem ganzen Wildwuchs eine definierte Verzeichnis-Struktur verborgen sein könnte. Die Antwort lautet: Teilweise. Einige Standards sind etwa in der Entwickler-Dokumentation festgelegt, andere lassen sich durch Vergleich verschiedener Geräte „erraten“.

Verzeichnis	Kommentar
Android/data/ <package_name>/	entspricht /data/data/<package_name>. Aktuelle Android-Versionen löschen dieses Verzeichnis bei Deinstallation der zugehörigen App.
Music/	Was der Medien-Scanner hier findet, stuft er als Musik ein
Podcasts/	... als Podcast
Ringtones/	... als Klingelton
Alarms/	... Alarmton
Notifications/	... Benachrichtigungston
Pictures/	Bilder (außer die der integrierten Kamera)
Movies/	Filme (außer die des integrierten Camcorders)
Download/	verschiedene Downloads
dcim/	Fotos/Videos der integrierten Kamera

Nicht immer wird sich an diese Strukturen gehalten – doch geben sie zumindest eine grobe Idee. Dummerweise machen die hier benannten Verzeichnisse meist weit weniger als die Hälfte der vorhandenen aus.

Welche Daten gespeichert werden

Android-Geräte speichern große Datenmengen – üblicherweise sowohl persönliche als auch geschäftliche Daten. Die primäre Quelle dieser Daten sind Apps – und für deren Herkunft gibt es eine Reihe von Quellen:

- Apps, die mit dem Android-System ausgeliefert werden
- Apps, die vom Hersteller vorinstalliert werden
- Apps, die der Netzanbieter vorinstalliert hat
- zusätzliche Google/Android-Apps
- Apps, die der Benutzer selbst (üblicherweise aus dem Market) installiert hat

Und was speichern all diese Apps auf dem Android-Gerät? Da wären beispielsweise:

- Textnachrichten (SMS/MMS)
- Kontakte
- Anruflisten
- Email-Nachrichten (Google, Yahoo, Exchange, ...)
- Instant Messenger / Chat
- GPS-Koordinaten
- Fotos/Videos
- Browser-Verlauf
- Such-Verlauf
- Wegbeschreibungen
- Daten von Facebook, Twitter und anderen sozialen Netzwerken
- Musiksammlungen
- Kalender-Termine
- Finanzinformationen
- Einkaufslisten / Shopping History
- File-Sharing

Alles keine großen Überraschungen – doch oft sind wir uns vieler Details nicht bewusst. Diese Datensammlung kann viel über den Besitzer des Gerätes aussagen – was in den falschen Händen durchaus unangenehme Folgen haben kann. Daher ist diesem Sachverhalt ein eigener Abschnitt gewidmet, der sich bereits weiter vorn in diesem Buch findet: *App-Sicherheit*. Dort finden sich auch weitere Details und Beispiele.

2.3 System-Info

Der Google Playstore bietet zahlreiche Tools, welche die verschiedensten Information zum System zu Tage fördern. Manche dieser Informationen möchte man gern ständig im Blick haben, andere benötigt man seltener. Zur ersten Kategorie gehören vielleicht Dinge wie CPU-Auslastung oder verfügbarer Speicher: Da bieten sich zweifellos Widgets an. Diese eignen sich allerdings weniger für ausführlichere Informationen (wie etwa eine Liste laufender Prozesse).

Es ist nicht einfach, alles eindeutig zu gruppieren – dazu gibt es zu viele Überschneidungen. Ich hoffe dennoch, dass mir eine passende Zusammenstellung gelungen ist.

Systeminfo-Widgets

Und schon beim ersten Tool scheitert es, da es nahezu alle Bereiche umfasst. Aber es ist sauber in einzelne Pakete gegliedert. Die Rede ist von *Elixir 2*, dessen Basis-Paket etwas weiter hinten unter *Ausführlichere System-Infos* vorgestellt werden soll. Sehr vorbildlich hat der Entwickler den Zugriff auf persönliche Informationen in ein **Personal Add-On** ausgegliedert; so sind die geforderten Permissions der **Elixir 2 Widgets** (Bild 2.3) zwar nicht wenige – dafür aber recht unbedenklich.



Elixir 2 Widgets

Der für dieses Kapitel interessante Teil hat im Screenshot einen blauen Hintergrund und zeigt wichtige Informationen zum System auf einen Blick. Dabei hat man die Auswahl aus einigen Datenquellen: Akku (Füllstand, Spannung, Temperatur), externer/interner Speicher, CPU (Auslastung und/oder Frequenz), RAM, Anzahl laufender Prozesse, Uptime, Signalstärke (Wifi, Mobilfunk), Traffic (Wifi, Mobilfunk) – aber auch (roter Bereich) Anzahl ungelesener Mails/Kurznachrichten, verpasste Anrufe und mehr. Und um dem nächsten Kapitel gleich vorzugreifen: Auch eine ganze Reihe von „Toggle-Widgets“ (also „Schnellumschalter“, siehe obere Bildhälfte) sind mit an Bord, wie etwa APN, Wifi, Wifi Hotspot (aka **Tethering**), Bluetooth, GPS, Flugzeugmodus und sogar SD-Mount sowie SD-Refresh (Media-Scan anstoßen) stehen hier – unter anderem – zur Auswahl. Und bei den Widgets stört es auch wenig, dass es wohl keine Unterstützung für die deutsche Sprache gibt: Ausgewiesen sind nämlich nur Englisch und Ungarisch.

Ein unheimlich erfolgreiches Päckchen, dieses *Elixir 2*. Das am besten bewertete Päckchen in diesem Bereich, nebenbei bemerkt. Und ich traue mich kaum zu schreiben, was denn wohl das zweitbestbewertete Päckchen sein könnte – das trägt nämlich den Namen *Elixir* und ist die Vorgänger-Version (bei der die Widgets noch nicht in einer separaten APK-Datei ausgeliefert wurden).



Bild 2.3: *Elixir 2* bietet Widgets für viele Einsatzgebiete

Auch das an dritter Stelle folgende *Mini Info* (Bild 2.4) fällt in diese Misch-Kategorie: Für den Home-Screen bietet es einige Widgets mit den wichtigsten Informationen wie Akku (Reststand, verbraucht, Spannung, Temperatur, Status), RAM/CPU (in Nutzung bzw. verfügbar) und Speicherplatz (intern/extern; belegt, frei, total). Die dahinterstehende App stellt dann bei Bedarf weitere Informationen zur Verfügung sowie eine Bar mit „Toggle-Widgets“. Die Info-Widgets lassen sich, wie auf dem Screenshot zu sehen, nach Gusto gruppieren. Ebenso ist das Festlegen eines Hintergrundes möglich: von völlig transparent über halbtransparent/Glas bis hin zur „Vollfarbe“.



Mini Info

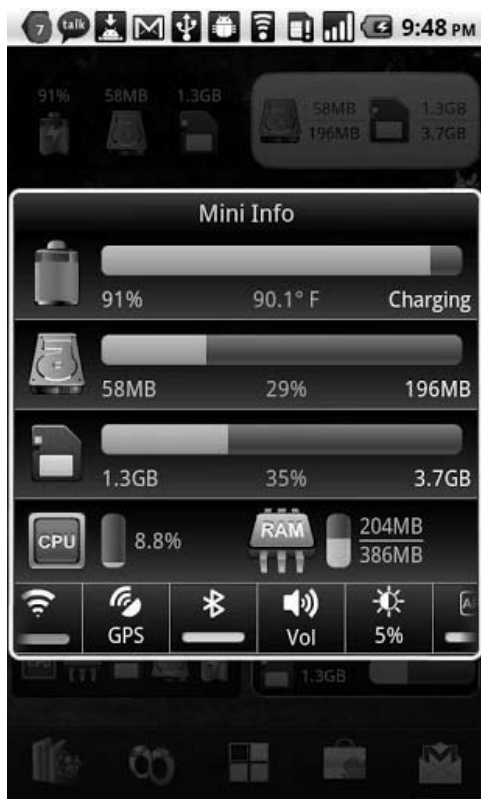


Bild 2.4: Mit *Mini Info* lassen sich die wichtigsten System-Informationen im Blick behalten

Zum Ausprobieren gibt es *Mini Info* gratis, der volle Funktionsumfang lässt sich per Donation (ca. anderthalb Euro) freischalten. Übrigens gibt es für diese App einen super Support mit kurzen Reaktionszeiten.

Auch wenn sich diese Apps wieder nicht ausschließlich dem Thema „Systeminfo-Widgets“ widmen, finde ich die Kombination sehr sinnvoll: Uhr und Wetter (im Stil von *HTC Sense*, daher auch der Name) und unmittelbar darunter die wichtigsten System-Infos eingeblendet – so kommt *Sense Analog Clock Widget 4x2* daher (Bild 2.5; auch in anderen Varianten mit 24-Stunden-Display oder im Glass-Look erhältlich). Ja, auch die Wettervorschau für die nächsten Tage ist integriert – doch da es hier ja um die Systeminfo-Widgets gehen soll: Das Wichtigste wird dargestellt (RAM, interner/externer Speicher, Temperatur und Akku-Stand), detailliertere Infos gibt es beim Antippen. Auch lässt sich konfigurieren, welche App beim Antippen der Stunden- oder der Minutenzahl geöffnet werden soll (Kalendarer und Wecker bieten sich hier an), sodass kein Platz „verschwendet“ wird.



Sense Analog
Clock Widget 4x2



Bild 2.5: *Sense Clock* blendet die wesentlichen Eckdaten gleich unter der Uhr ein

Eine Auswahl weiterer Widget-Sammlungen finden sich in der Übersicht bei AndroidPIT.



<http://www.androidpit.de/de/android/forum/thread/410598/>

Schnellumschalter

Hier könnte ich es mir jetzt einfach machen und schreiben: „Siehe oben“ – zumindest die vorderen Plätze sind sogar identisch (*Elixir 2* und *Elixir*). Ebenso ist oben genanntes *Mini Info* recht weit oben mit dabei. Aber einige Kandidaten haben sich speziell auf das „schnelle Umschalten“ spezialisiert und sollen daher auch in diesem Abschnitt genannt werden.

So nimmt etwa **MySettings** (Bild 2.6) vergleichsweise viel Platz ein, ist aber nach den beiden *Elixieren* in dieser Kategorie die am besten bewertete App. Wer genau hinschaut, erkennt hier sogar noch grundlegende System-Infos, die am oberen Rand eingebettet werden. Mit dieser App lässt sich nicht nur schnell umschalten, auch Helligkeit und diverse Lautstärke-Regler lassen sich mit ihr schnell justieren. Somit ist es eigentlich eine Kreuzung aus „Schnellumschalter“ und „Schnellkonfigurator“. Wie wir nun bereits mehrfach gesehen haben, sind die Grenzen zwischen den einzelnen Bereichen recht fließend.

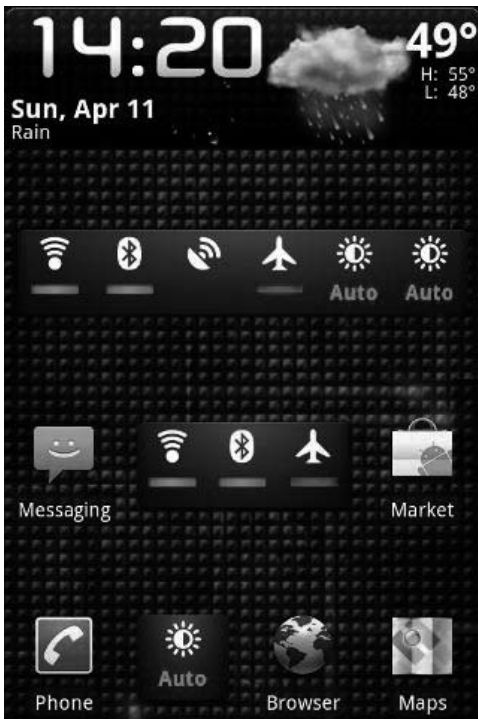


MySettings

Bild 2.6: **MySettings** ist eine Kreuzung aus Schnellumschalter und Schnellkonfigurator

Eine feine Sache ist auch **Dazzle** (Bild 2.7). Hier lassen sich beliebige Kombinationen aus „Toggles“ in einem Widget kombinieren – auch sieben Schalter in einer Leiste (4x1 Widget) sind kein Problem in der Darstellung (anders aussehen mag das in Bezug auf die Treffsicherheit von Wurstfingern). Was auf dem Screenshot auch sehr schön zu sehen ist: Man kann durchaus mehrere Widgets anfertigen, die unabhängig voneinander konfigurierbar sind (die *Dazzle*-Widgets sind auf dem Screenshot ausschließlich die mit dem schwarzen Hintergrund). Das ergibt größtmögliche Flexibilität.

Darüber hinaus geht hier mehr als bloßes „An“ und „Aus“: Auf Wunsch gibt es auch „Pop-Up-Schieberegler“ etwa für stufenlose Regelung der Bildschirm-Helligkeit oder Klingelton-Lautstärke. Für den Klingelton ist auch ein Multi-Schalter möglich ist: An/Aus/Vibrieren plus Knopf für Benutzerwert. Wer mag, kann auch einfach den Mobilfunk abschalten – etwa um ungestört von Anrufen und eingehenden Kurznachrichten im WLAN zu surfen.



Dazzle

Bild 2.7: Mit **Dazzle** lassen sich verschiedene Schnellumschalter beliebig kombinieren

Eine der beliebtesten Lösungen in diesem Umfeld ist sicher nicht ohne Grund **Widgetoid 2**. Hier lässt sich alles bis ins Feinste anpassen (von Hintergrundfarbe und Transparenz über benutzerdefinierte Farben und Label, unterschiedliche Widget-Größen (bis zu 10 Schaltflächen auf einem Widget) bis hin zu eigenen Hintergrundbildern für die Widgets) und die Widget-Auswahl enthält neben den „üblichen Verdächtigen“ auch Dinge wie das Neueinlesen der SD-Karte, Reboot (bei gerooteten Geräten gar mit Auswahl aus Recovery, Bootloader, Fastboot, Normal und Herunterfahren), Tethering (WLAN/USB), beliebige App-Verknüpfungen oder gar Kontakte (optional mit Popup-Auswahl aus Anrufen, SMS, E-Mail).



Widgetoid 2

Man kann sich auf den Widgets auch Dinge wie Akkustand und -temperatur, Speicher oder RAM anzeigen lassen.

Die Krönung ist jedoch: Das Ganze lässt sich auch in die **Notification Area** einbauen (siehe Bild 2.8)! Auf diese Weise hat man seine Schnellumschalter jederzeit durch einfaches Herunterziehen der Statusleiste im Zugriff – egal, auf welchem Screen oder gar in welcher App man sich gerade befindet. So dürfte **Widgetoid 2** die am umfangreichsten anpassbare App in diesem Bereich sein.



Bild 2.8: *Widgetoid 2* lässt sich auch in den Benachrichtigungs-Bereich integrieren

Damit könnte nun die Vorstellung der Schnellumschalter wirklich enden. Und das tut sie auch – mit dem Hinweis, dass sich bei Bedarf weitere Apps in der Übersicht bei Android-PIT finden.



<http://www.androidpit.de/de/android/forum/thread/410407/>

Ausführlichere System-Infos

Auch an dieser Stelle geht der Verweis zuerst „nach oben“: Wie schon bei den Widgets steht hier ein *Elixir* an erster Stelle, und zwar die Basis-App *Elixir 2*, die – wie in Bild 2.9 zu sehen – Informationen zu vielen Bereichen zur Verfügung stellt. Dazu zählen u. a. Geräte-Informationen wie Akku (Ladezustand, Spannung/Strom, Temperatur), interner und externer Speicher (insgesamt/frei, wo eingebunden), CPU (Auslastung, Frequenz), RAM (insgesamt/frei), Telefonie (Netzwerk-/Telefonmodus, Provider, APN), installierte Anwendungen (wo installiert, wieviel Platz belegt die App, wieviel ihre Daten, welche Version), welche Prozesse/Services laufen (und verwenden wieviel RAM/CPU etc.), aber auch Daten der Sensoren. Ebenso lassen sich diverse Systemeinstellungen (wie etwa Bildschirmhelligkeit oder Lautstärke) anpassen oder Aktionen wie Cache-Bereinigung, SD-Karte ein-/ausbinden oder Bluetooth-Scan durchführen. Als würde das noch nicht reichen, greift die App auch noch in das Kapitel *Logcat* und zeigt die Systemlogs an. Großer Rundumschlag – oder Schweizer Offiziersmesser. Und dabei habe ich noch lange nicht alles aufgezählt.



Elixir 2

Bild 2.9: *Elixir 2* bietet zahlreiche Systeminformationen

Recht umfangreiche Informationen zum System stellt auch **Android System Info** (Bild 2.10) bereit. Diese bestehen u. a. aus einem „Dashboard“ mit den wichtigsten Eckdaten, einem Task-Manager, der sowohl Task-Switcher als auch Task-Killer beinhaltet, einer Anwendungs-Verwaltung für die installierten Apps, einem farblich aufbereiteten System-Log (noch jemand, der dem Kapitel **Logcat** vorgreift) sowie weiteren Informationen rund um das System. Etliche Nutzer berichten, was ihnen besonders gefällt: zahlreiche Informationen und doch übersichtlich aufbereitet. Entsprechend weit oben ist es auch auf der Bewertungsliste platziert: Durchschnittlich 4,6 Sterne bei über 20.000 Bewertungen, trotzdem hinter *Elixir 2*, welches über 4,8 Sterne durchschnittlich erhielt.



Android System Info

Vom Aufbau her vergleichbar wäre **OS Monitor**, bringt allerdings noch ein paar Schmankehl mit: etwa die auf dem Screenshot zu sehende „grafische WhoIs-Abfrage“: Wohin hat sich diese App gerade verbunden? Aha.

Im Hintergrund erkennt man bei genauerem Hinsehen in Bild 2.11 noch die „Reiterlein“. Hinter selbigen verbergen sich eine Prozessliste (die sich nach verschiedenen Kriterien

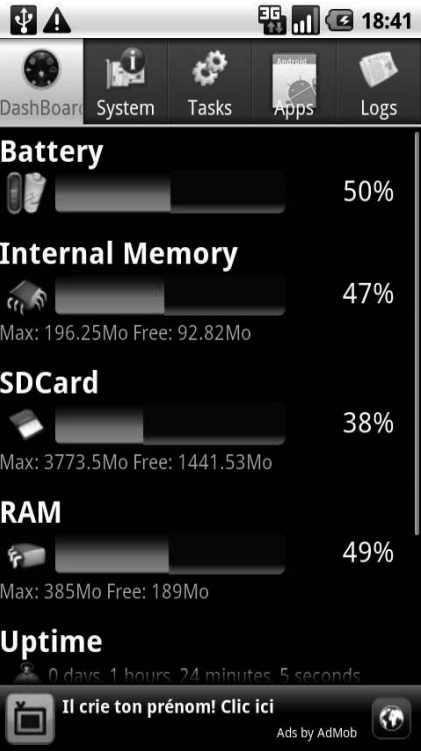
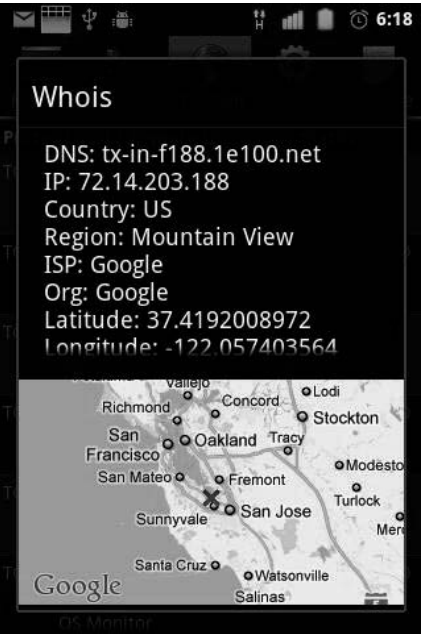


Bild 2.10: Neben einem Dashboard bietet **Android System Info** auch Zugriff auf zahlreiche Details



OS Monitor

Bild 2.11: **OS Monitor** gibt auch Einblick in den Netzwerk-Verkehr

wie beispielsweise CPU oder Speicherverbrauch sortieren lässt und auch einen Task-Killer beinhaltet), eine Übersicht über verfügbare Netzwerk-Interfaces (mit – sofern verfügbar – Details zur **MAC-Adresse**, zugeteilten IP, sowie bereits übertragenen Datenmenge), aktuelle Datenverbindungen (welche App wohin, mit welchem Netzwerk-Protokoll?), eine Zusammenfassung „verschiedener“ Informationen (CPU, Akku, Speicher) sowie – ja, auch hier wieder – ein farblich aufbereitetes Systemlog.

Zusätzlich lässt sich die CPU-Auslastung mit einem kleinen Icon in der Statusleiste einblenden – entweder einmalig manuell oder automatisch bei jedem Systemstart aktiviert. Wenn der Androide gerootet ist, lässt sich auch die Taktfrequenz der CPU anpassen. Bei 170kB *.apk*-Datei (installiert gut 300kB) ist die App mit diesen Leistungsmerkmalen recht kompakt geraten. Die Permission-Liste ist ebenfalls sauber, und die Bewertungszahl (mit durchschnittlich 4,5 Sternen bei fast 5.000 Bewertungen) ist topp.

Weitere Apps zur Beschaffung von System-Informationen finden sich in der Übersicht bei AndroidPIT. Ein paar grundlegende Informationen findet man übrigens auch mit Bordmitteln, indem man vom Home-Screen aus über *Menü* → *Einstellungen* geht und *Telefoninfo* auswählt.



<http://www.androidpit.de/de/android/forum/thread/410598/>

System Logs

Spätestens, wenn etwas nicht so tut, wie es sollte, kommt die Frage auf: „Was geht da eigentlich ab?“ Neugierige, Entwickler und auch technisch Interessierte stellen diese Frage selbst dann, wenn alles reibungslos läuft.

Auskunft darüber geben die Log-Dateien des Systems – von denen es in der Tat einige gibt. Und ebenso gibt es eine ganze Reihe von Möglichkeiten, an ihre Inhalte zu kommen. Einige davon sollen hier vorgestellt werden. Doch bevor es an die Details geht, möchte ich eine grobe Übersicht voranstellen: Auf welche Arten lässt sich auf diese System-Protokolle zugreifen?

Methode	Vorteile	Nachteile
Per App	Kein weiteres Gerät und keine spezielle Software auf dem Arbeitsrechner notwendig	kleiner Bildschirm (insbesondere auf Smartphones), eingeschränktes Multitasking
Via ADB	Bequemes Arbeiten vom PC aus, einfaches Multitasking	PC mit installiertem SDK notwendig
Via SSH	Bequemes Arbeiten vom PC aus, einfaches Multitasking	?

Zugriff per App

Ab und an benötigt auch der einfache Anwender einen Auszug aus den System-Logs, etwa wenn eine App sich „seltsam verhält“ oder gar nachvollziehbar abstürzt und man dies dem Entwickler mitteilen möchte. Der nämlich freut sich über derartige Details. Weiter oben habe ich bereits aufgezeigt, dass einige Apps diese Informationen sehr wohl anzeigen, nur wie bekommt man selbige dann zum Entwickler?

Die bekannteste Antwort darauf heißt sicher **aLogcat** (Bild 2.12), ist mit 4,6 Sternen bei über 1.500 Bewertungen recht beliebt und sollte auf keinem Androiden fehlen. Diese App startet man, leert die Einträge kurz über den abgebildeten „Clear Log“-Button, provoziert den Fehler in der fraglichen App, kehrt zu aLogcat zurück, drückt auf „Pause“ (da wo jetzt „Play“ steht) – und nun hat man die Wahl, den Log-Ausschnitt mit „Save Log“ auf die SD-Karte oder über den „Send“-Button per Mail direkt zum Entwickler zu befördern. Das schaffen auch technisch weniger Versierte!

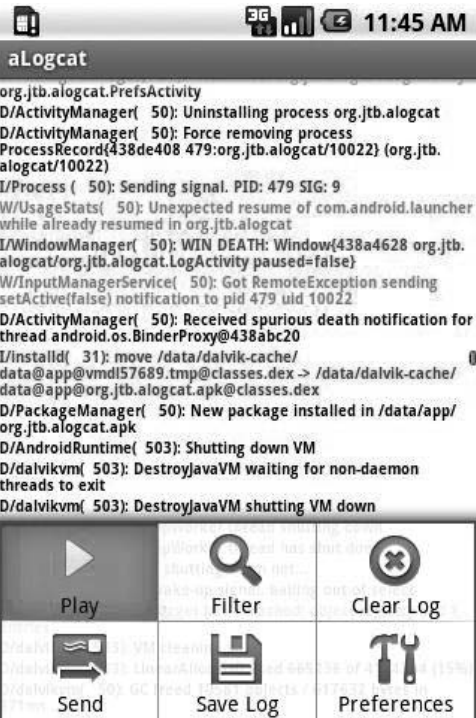


Bild 2.12: aLogcat ist ein beliebtes und praktisches Tool zum Zugriff auf System-Logs

Alternativ wäre noch der **Log Collector** zu nennen, der ähnlich funktioniert, oder auch der in Bild 2.13 abgebildete **Bug Reporter**, der zusätzlich zum Auszug aus den Systemlogs auch noch Informationen zum verwendeten Android-System sammelt und in die Mail an den Entwickler einschließt – das erspart das mühsame manuelle Zusammensuchen und stellt sicher, dass man kein wesentliches diesbezügliches Detail vergessen hat.

Weitere mögliche Alternativen findet man, indem man erstgenanntes *aLogcat* bei AndroidPIT aufsucht und in die Liste vergleichbarer Apps schaut. Da fast alle gleich arbeiten und aussehen, habe ich dazu keine separate Übersicht erstellt.



Log Collector



Bug Reporter



Bild 2.13: Bug Reporter

ist hilfreich, um einen Entwickler schnell mit den wichtigsten Informationen zu versorgen

Zugriff via ADB oder SSH

Doch das ist bei Weitem nicht alles, was das System an Logs zu bieten hat, sondern lediglich das, was dem Anwender recht bequem zur Verfügung steht. Wer gern noch etwas tiefer graben möchte, hat dazu durchaus die Möglichkeit: entweder mit einer Terminal-App direkt auf dem Androiden oder aber bequemer vom PC aus, was jedoch die Installation der Android Entwicklungs-Umgebung (**SDK**) – oder alternativ den Einsatz eines **SSH**-Servers auf dem Androiden – erforderlich macht. Bevor ich also auf die einzelnen Logs eingehe, kurz ein paar Worte dazu.

Bei auf dem Arbeitsrechner installiertem SDK und einem mit aktiviertem USB-Debugging (dies lässt sich im Systemmenü des Androiden unter *Anwendungen* → *Entwicklung* ein- und ausschalten) per USB-Kabel angeschlossenen Android-Gerät lässt sich über **ADB** auf letzteres zugreifen. Der Name „Android Debug Bridge“ legt bereits nahe, dass ADB hauptsächlich zur Entwicklung gedacht ist. Um Befehle vom Arbeitsrechner aus direkt auf dem Androiden ausführen zu können, stellt das SDK den Befehl `adb shell` zur Verfügung. Wer also Folgendes bequem über die ADB ausprobieren möchte, setzt jedem Befehl einfach ein `adb shell` voran – etwa `adb shell logcat`. Die Ausgabe erfolgt dann natürlich im Terminal-Fenster des Arbeitsrechners.

dmesg

Was wird nun vom Android-System eigentlich alles protokolliert? So allerhand. Nur wird es nicht lange aufgehoben. Die meisten Protokolle liegen auf einem temporären Dateisystem (*tmpfs*), das bei Systemstart im RAM angelegt wird. Nach einem Neustart des Androiden sind also alle zuvor angelegten Einträge weg. Dafür werden aber neue geschrieben – und zwar bereits wenn das System hochfährt. Da Android auf einem Linux-Kernel läuft, kommt Linux-Anwendern natürlich sofort der Befehl `dmesg` in den Sinn, und tatsächlich findet sich das auch hier wieder. Da die Ausgaben recht umfangreich sind, empfiehlt sich die Umleitung in eine Datei, etwa wie folgt: `dmesg > /mnt/sdcard/dmesg.log`.

```
$ dmesg
<6>[82839.126586] PM: Syncing filesystems ... done.
<7>[82839.189056] PM: Preparing system for mem sleep
<4>[82839.189361] Freezing user space processes ... (elapsed 0.05
seconds) done.
<4>[82839.240661] Freezing remaining freezable tasks ... (elapsed
0.00 seconds) done.
<7>[82839.242279] PM: Entering mem sleep
<4>[82839.242889] Suspending console(s) (use no_console_suspend to
debug) <7>[82839.252410] vfp_pm_save_context: saving vfp state
<6>[82839.252716] PM: Resume timer in 26 secs (864747 ticks at 32768
```

```
ticks/sec.)
<6>[82842.091369] Successfully put all powerdomains to target state
<6>[82842.092468] wakeup wake lock: wifi_wake
<snip>
```

Wie bei den meisten anderen Protokoll-Dateien handelt es sich auch bei `dmesg` um einen „Ringpuffer“ mit fester Größe: Ist er voll und muss etwas Neues geschrieben werden, dann fliegt etwas Altes raus. `dmesg` ist ja keinesfalls ein „Boot-Log“, sondern vielmehr die Log-Datei des Kernels – und der läuft ständig im Hintergrund. Je länger also der letzte Bootvorgang her ist, desto wahrscheinlicher sind auch die entsprechenden Einträge bereits durch neuere Ereignisse überschrieben worden.

logcat

Bereits im Zusammenhang mit einigen grafischen Tools wurde `logcat` genannt. An der Kommandozeile lässt sich diesem noch Einiges und viel präziser entlocken. Eine ausführliche Beschreibung dieses Befehls ist auf der Hilfe-Seite der Android-Entwickler-Website zu finden – dennoch hier ein paar kurze Hinweise.

Ein kleines Problem zeigt sich nämlich gleich beim ersten Aufruf:

```
$ logcat
Unable to open log device './dev/log/main': Permission denied
```

Anders als mit den oben genannten Apps scheint der `shell`-User also nicht so ohne Weiteres Zugriff auf `logcat` zu erhalten – zumindest bei Zugriff über **SSH** benötigt man also **root-Rechte**. Dann funktioniert es aber:

```
$ su # logcat
----- beginning of /dev/log/system
<snip>
D/WifiWatchdogService( 3457): (android.server.ServerThread) IzzySoft
(24:65:11:67:d7:6d) does not require the watchdog
I/ActivityManager( 3457): Starting: Intent { act=android.settings.
WIFI_SETTINGS cat=[android.intent.category.DEFAULT] flg=0x10000000
cmp=com.android.settings/.wifi.WifiSettings } from pid 3529
W/InputManagerService( 3457): Starting input on non-focused client
com.android.internal.view.IInputMethodClient$Stub$Proxy@409f6128
(uid=1000 pid=2760)
<snip>
```


Über den Parameter `-b` lässt sich der Puffer angeben, aus dem man Informationen erhalten möchte. So liefert beispielsweise ein `logcat -b events` Daten aus dem Ereignis-Protokoll, während `logcat -b radio` Details zum „Radio“ (also dem Mobilfunk-Element) preisgibt. Auch diverse Einstellungen lassen sich mit diesem Befehl steuern – etwa die Größe des zu verwendenden Ringpuffers. Sie gelten natürlich nur bis zum nächsten Gerätestart.

```
$ su # logcat -b events
I/am_create_service( 3457): [1085416560,nitro.phonestats/.widget.Wid
getProvider4x1$WidgetUpdateService4x1,,3721]
I/am_destroy_service( 3457): [1085416560,nitro.phonestats/.widget.Wi
dgetProvider4x1$WidgetUpdateService4x1,3721]
I/notification_cancel( 3457): [nitro.phonestats,4,0]
I/db_sample( 4002): [/data/data/com.lbe.security.lite/databases/
lbe_trafficmon.db,INSERT OR REPLACE INTO uid_traffic(wifitx, wifirx,
date_uid, ce,0,com.lbe.security.lite,1]
I/force_gc( 3721): bg I/dvm_gc_info( 3721): [8099846449757718054,-
9031259007116011474,-4008901822536468439,0]
<snip>
```

Jede Zeile der Logcat-Ausgabe beginnt mit einem Loglevel-Hinweis, gefolgt von einem Schrägstrich, gefolgt vom Ursprung des Eintrags – beispielsweise

`D/WifiWatchdogService( 3457)`. Daran schließt sich sodann die eigentliche Meldung an. Folgende Log-Level gibt es: Verbose, Debug, Info, Warning, Error, Fatal, Silent. Der Wert in Klammern gibt die Prozess-ID an, sodass auch Querverweise zu anderen Protokollen möglich sind.

dumpsys und dumpstate

Diese beiden Befehle geben ausführliche Informationen zum System: Dienste, Speicher, Broadcasts, anstehende Intents, Activities, Prozesse, Account-Informationen, Informationen über das Gerät, Build, Radio, Netzwerk, Kernel-Details ... Auch hier empfiehlt sich, die Ausgaben in eine Datei schreiben zu lassen, da sie überaus umfangreich sind.

Für beide Befehle werden keine root-Rechte benötigt – jedoch fehlen bei Ausführung ohne selbige einige Details:

```
$ dumpsys
Currently running services:
  LocationProxyService
  SurfaceFlinger
```

```

    accessibility
    account activity
<snip>
DUMP OF SERVICE account:
Accounts: 1
    Account {name=xxxxxxx@googlemail.com, type=com.google}
<snip>
DUMP OF SERVICE alarm:
Permission Denial: can't dump AlarmManager from from pid=7274,
uid=10038
<snip>
DUMP OF SERVICE batteryinfo:
Battery History:
    -10h32m25s939ms 099 23c30040 status=discharging health=good
    plug=none temp=280 volt=4117 +scre en +wifi +wifi_running +wifi_
    full_lock +wifi_scan_lock +wake_lock +sensor signal_strength=great
    -10h32m19s441ms 099 03c10040 -screen -wake_lock
<snip>

$ dumpstate
=====
== dumpstate: 2012-08-18 23:39:53
=====

Build: Gingerbread GWK74 - CyanogenMilestone2
Bootloader: 0x0000
Radio: unknown
Network: E-Plus
Kernel: Linux version 2.6.32.9-g5db7937 (a17140@zch68lnxdroid63)
(gcc version 4.4.0 (GCC) ) #1 PREEM PT Fri Sep 16 17:57:00 CST 2011
Command line: (unknown)

----- MEMORY INFO (/proc/meminfo) -----
MemTotal: 487344 kB
MemFree: 10436 kB
Buffers: 14136 kB
Cached: 145460 kB
<snip>

```

Unschwer zu erkennen, dass sich hier allerhand über System, Konfiguration, Dienste und Vieles mehr in Erfahrung bringen lässt.

bugreport

Frage: Was mag sich wohl hinter einem Befehl mit diesem Namen verbergen? Antwort: alles obige für Tippfaule. Gibt man `bugreport` im Terminal (oder `adb shell bugreport` via ADB) ein, flattern die Zeilen nur so über den Bildschirm – hier sollte also auf jeden Fall die Ausgabe in eine Datei umgeleitet werden (`bugreport > /mnt/sdcard/bugreport.txt`). Das Ergebnis sind dann alle von `logcat`, `dumpsys` und `dumpstate` gesammelten Informationen in einem schönen Bugreport für den Entwickler – also genau das, was auch die oben beschriebene App *Bug Reporter* erzeugt.

Andere Logdateien

Außer den bislang genannten Standard-Logs gibt es noch einige Verzeichnisse, in denen sich Log-Dateien finden lassen. Da diese durchaus von Gerät zu Gerät (und auch zwischen verschiedenen Android-Versionen) unterschiedlich sein können, sind nicht alle hier genannten Verzeichnisse auf jedem Gerät vorhanden. Die mit „AOSP“ gekennzeichneten sollten jedoch zum Standard gehören. Aber selbst wenn das Verzeichnis existiert, kann es durchaus auch leer sein.

`/data/anr`: Einige **Trace-Logs** landen u. U. hier (bei Application Not Responding, auch als „Force-Close“ oder „Schließen erzwingen“ bekannt).

`/data/dontpanic` (AOSP): Crash-Logs mit **Traces**. Im Falle einer auftretenden Kernel-Panik finden sich hier zwei Dateien: `apanic_threads` verzeichnet den zu diesem Zeitpunkt aktiven Prozess/Thread, `apanic_console` enthält zusätzliche Informationen wie Traces und Register.

`/data/kernelpanics` (AOSP): Log-Einträge bei sog. „Kernel-Panic“.

`/data/panic/panic_daemon.config`: Konfigurations-Datei für den Panic-Daemon. Wenn unterstützt, lässt sich hier festlegen, wohin Panic-Logs bei manueller Auslösung (über Geräte-spezifische Tastenkombinationen) geschrieben werden (oft `/sdcard/panic_data/`).

`/data/panicreports`: Weitere Panik-Protokolle werden bei einem „Not-Halt“ hier abgelegt (AOSP).

`/data/tombstones`: Lustig sind sie ja, die AOSP-Entwickler: Auf das Grab (englisch „tomb“) kommt ein Stein (englisch „stone“), also ein Grabstein („tombstone“), damit man sich an den Toten erinnert. Stirbt also ein Prozess unerwartet (auch als „Absturz“ oder „Crash“ bekannt), kann er sich auch so einen „Grabstein bestellen“, der dann Informationen zu seinem Ableben enthält. Auf Linux/Unix-Systemen nennt man dies „Core Dumps“.

Monitoring

Fast 5.000 Nutzer bewerteten es mit durchschnittlich 4,7 Sternen, es kostet gut zwei Euro: **SystemPanel** scheint mir hier die App der Wahl, um einen „Bösewicht“ aufzuspüren. Beispielsweise wenn man wissen möchte, wer einem da gerade den Akku leer genuckelt hat: Vor vier Stunden war er noch randvoll, und jetzt ist die Hälfte verschwunden? **SystemPanel** hat da sicher die passenden Details zur Hand, wie in Bild 2.14 ersichtlich.



SystemPanel

Die Auswertung von oben nach unten: Zwischen 18 und 20 Uhr hat Google Maps die CPU mit ca. 5% Beschlag belegt – davor und danach gar nicht („Process CPU Activity“). Eine externe Stromversorgung (Ladekabel) war in diesem Zeitraum nicht angeschlossen, sondern erst wieder ab ca. 21 Uhr („Charging“). Ebenfalls im Zeitraum von 18 bis 20 Uhr verlor der Akku etwa die Hälfte seiner Ladung („Battery Charge“), was sich so ziemlich mit der Aktivität von Maps deckt. Das Ganze scheint außerdem größtenteils „im Hintergrund“ geschehen zu sein, denn laut „Device Usage“ war der Anwender selbst im gleichen Zeitraum weniger aktiv. Da hätten wir also den Verursacher ziemlich genau identifiziert, oder? Doch halt: Die gesamte CPU-Auslastung („CPU Activity“) lag im fraglichen Zeitraum bei über 10%, also muss wohl noch jemand beteiligt sein ...



Bild 2.14: **SystemPanel** hilft bei der Suche nach Ressourcen-Fressern

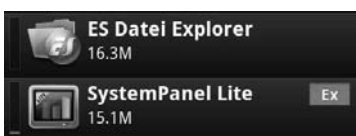


Bild 2.15: Der kleine Balken links zeigt, wie viele CPU-Zyklen eine App verbraucht hat

Eine derartige Auswertung ist nur in der Vollversion möglich, die das „Protokollieren“ erlaubt (also im Hintergrund die Daten bis zu einer Woche lang festhält). Neben diesem System-Monitor bietet *SystemPanel* noch Geräte-Information, einen Task-Manager sowie einen App-(Un-)Installer. Einen ersten Eindruck kann man sich natürlich mit der Lite-Version verschaffen.

Und auch mit der Lite-Version lässt sich bereits Einiges anstellen. Auf der Suche nach Ressourcen-Fressern fällt gleich in der App-Liste der kleine senkrechte Balken links der App-Namen auf (siehe Bild 2.15): Je höher dieser gefüllt ist, desto mehr CPU-Zyklen hat dieser Prozess während seiner Laufzeit beansprucht. Ist der Balken besonders hoch und dies durch Art und Einsatz der App nicht gerechtfertigt? Dann wird es vielleicht Zeit, sich nach einer Alternative umzusehen.

Der nächste Blick gilt der Tatsache, welche App die CPU besonders lange mit Beschlag belegt hat. Dazu gibt die Übersicht der Top-Apps nach CPU (Bild 2.16) Auskunft. Eine App, die man nur gelegentlich verwendet und die (eigentlich) in der restlichen Zeit auch keine Hintergrund-Aufgaben durchzuführen hat, sollte hier nicht auftauchen. Ansonsten gilt gerade Gesagtes: Ist man als Anwender nicht selbst daran Schuld (es könnte ja auch eine Fehlkonfiguration vorliegen oder die ungewünschte Hintergrund-Funktion lässt sich etwa in der App selbst deaktivieren): Der Playstore bietet in der Regel genügend ähnliche Apps an – sofern der Entwickler der App nicht Abhilfe schaffen kann.



Bild 2.16: *SystemPanel*: Apps nach CPU-Verbrauch

Wonach könnte man noch schauen? Etwa nach dem Speicherverbrauch. Verbraucht eine App viel Speicher, heißt dies natürlich nicht automatisch, dass da etwas schief geht: Die Sache kann durchaus einen guten Grund haben. Doch der von einer App belegte Speicher steht anderen Apps nicht mehr zur Verfügung – und wird der Speicher knapp, bremst dies das System aus. Die Relationen sollten also schon stimmen: Verbraucht etwa eine einfache Stoppuhr mehr Speicher als eine Office-Suite, passt definitiv etwas nicht zusammen.

Ähnliches wie das nun ausführlich behandelte *SystemPanel* bietet auch **System Tuner** (Bild 2.17). Diese App kann ebenfalls Aktivitäten im Hintergrund aufzeichnen und für eine spätere Analyse zur Verfügung stellen, RAM und Speicherdetails anzeigen, hat einen Task-Manager an Bord und sogar einen Terminal-Emulator, sodass man Befehle direkt an der Kommandozeile absetzen kann. Letzteres klingt ein wenig „nerdy“? Auf gerooteten Geräten lässt sich mit *System Tuner* auch der Cache der SD-Karte anpassen, der **OOM-Killer** konfigurieren, die CPU tweaken – man kann gar System-Apps in den „User-Space“ verschieben oder gleich ganz deinstallieren. Das ist jetzt „nerdy“...



System Tuner

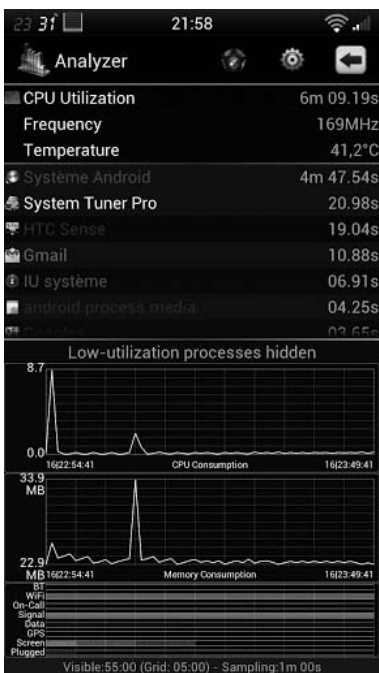


Bild 2.17: *System Tuner* hat neben dem Monitoring auch weitere Helferlein an Bord

Mit dabei ist hier auch ein Widget, welches die wesentlichsten Eckdaten (CPU, RAM, Speicher) anzeigen kann. Auch einige Aktivitäten (Monitoring starten/stoppen, Task-Manager/Analyzer/Einstellungen öffnen) lassen sich von diesem aus steuern.



BetterBatteryStats

Weitere interessante Daten stellt auch **BetterBatteryStats** (Bild 2.18) bereit. So bringt diese App etwa die *WakeLock*-Statistiken zurück, die bis einschließlich Froyo zum Bordgepäck gehörten. Der Name suggeriert es bereits: Hier wird jemand in den Wachzustand gesperrt – und zwar die CPU. Fordert also eine App ein *WakeLock* an (und erhält es zugeteilt), kann sich die CPU nicht schlafen legen, solange dieser aufrecht erhalten wird. So etwas schlägt sich natürlich nicht zuletzt im Akku-Verbrauch nieder.

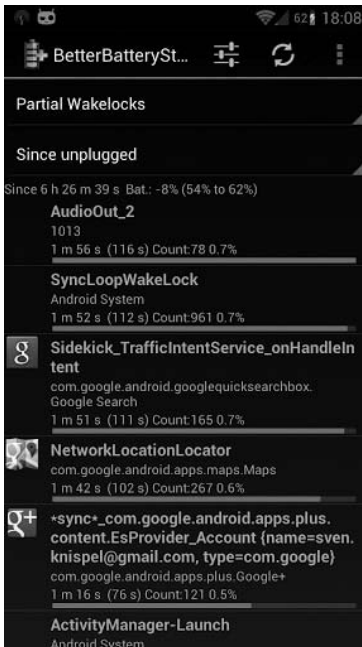


Bild 2.18: *BetterBatteryStats* verrät, wer das Gerät wachgehalten hat

BetterBatteryStats verrät uns also, welche Apps sich hier (aber auch in weiteren Dingen, die zum Akkuverbrauch beitragen) schuldig bekennen müssen. Dazu muss *BetterBatteryStats* selbst natürlich im Hintergrund mitlaufen – denn wie sonst soll die App an eben diese Daten kommen?

Auf zwei Dinge sollte hier besonders geschaut werden: Gleich auf der Startseite der App findet sich der Abschnitt *Deepsleep* („Tiefschlaf“). Wer hat hier besonders viel CPU verbraucht? Der ist ein Kandidat zum Löschen/Ersetzen, Deaktivieren des automatischen Startens bzw. Abstellen/Herunterregeln der automatischen Synchronisation. Schwieriger wird es bei Einträgen wie *Moderate Signal* (kein optimaler Netzempfang), *Wifi On* oder *Wifi Running* (WLAN): Das lässt sich nicht eben mit einer anderen App ersetzen. Lösungen gibt es dafür trotzdem, wie unter Abschnitt 3.4 bei *Automatische (De)Aktivierung* beschrieben ist.



Ein weiterer Punkt sind die bereits erwähnten Partial Wakelocks, wie in Bild 2.18 zu sehen. Hier verbergen sich die Bösewichter, die der CPU schlaflose Tage und Nächte bereiten. Interessanter Kandidat im Screenshot: *NetworkLocationLocator*. Das ist der Dienst von Google Maps, der überwacht, wo sich der Androide (und somit i. d. R. sein Besitzer) wann aufhält, und diese Informationen im **Location Cache** ablegt, um sie später an Google zu übertragen. Wie man sieht, ist der an kurzer Akku-Laufzeit nicht gerade unschuldig.

Da wir gerade beim Monitoring sind: Interessant wären sicher auch Informationen darüber, welche App wann im Internet wohin unterwegs war. Diese Funktionalität bietet unter anderem die App *DroidWall*, auf die ich bereits zuvor beim Thema *Firewalls* näher eingegangen bin. Für Bluetooth-Aktivitäten trifft das in gleicher Weise auf *Bluetooth Firewall* im selben Abschnitt zu.

2.4 Konfiguration

*Über sieben Brücken musst Du geh'n,
Und an mehr als sieben Schräubchen dreh'n ...*

Das Problem dabei ist häufig: Welche Schräubchen, und wo sind sie zu finden? Einige davon möchte ich im Folgenden kurz benennen:

Konfiguration mit Bordmitteln

Für die grundlegenden Dinge muss man nicht gleich auf zusätzliche Apps zurückgreifen. Ein wenig „Graben“ mit den Bordmitteln fördert so Manches zu Tage, dessen Existenz man nicht einmal geahnt hätte. Eine gute Empfehlung bei Geräte- bzw. ROM-Wechsel ist daher: Erst einmal ganz systematisch das gesamte Einstellungs-Menü durchgehen und schauen, was so alles dazugekommen ist. Oder verschwunden, auch das kommt vor: So manche sinnvolle und wünschenswerte Einstellung hat Google da mit der Zeit wieder „wegoptimiert“.

Die folgende Kurzübersicht orientiert sich an den Systemeinstellungen, die Froyo (Android 2.2) anbietet – mit dem einen oder anderen Schwenk nach oben oder unten. In diese Einstellungen gelangt man, indem man vom Home-Screen ausgehend die „Menü-Taste“ drückt und im sich öffnenden Menü den Punkt „Einstellungen“ (bzw. „Systemeinstellungen“, „Settings“, „System Settings“ – bei verschiedenen Herstellern bzw. Spracheinstellungen kann das natürlich leicht variieren) auswählt. Diese Stelle soll im Folgenden als Ausgangspunkt dienen – denn hier folgen die einzelnen „Sektionen“, deren Name (jedenfalls meistens) aussagekräftig in Bezug auf die dahinter verborgenen Einstellungen ist:

Drahtlos und Netzwerke

Eindeutig: Hier funkt es. Zumindest kann man hier die entsprechenden Einstellungen tätigen. Mit den „Häkchen“ (siehe Bild 2.19) lassen sich einzelne Features (de-)aktivieren. So sorgt der *Flugzeugmodus* für Funkstille: Keine mobilen Daten, kein Telefon – alles, was die empfindliche Bordelektronik stören könnte, wird damit auf einen Schlag abgeschaltet. Damit kann man den Androiden auch an Bord eines Flugzeugs nutzen – etwa um eBooks zu lesen. Handelt es sich um eine fortschrittliche Fluggesellschaft, die WLAN an Bord anbietet, so lässt sich Letzteres auch nutzen, indem man WLAN im Flugzeugmodus separat aktiviert.



Bild 2.19: Android-Systemeinstellungen: *Drahtlos und Netzwerke*

Hinter den Feldern mit dem auf der Spitze stehenden dreieckigen Symbol verstecken sich weitere Konfigurations-Bildschirme: So kann man unter „Wifi-Einstellungen“ etwa in Reichweite befindliche WLAN-Netze anzeigen lassen, sich mit selbigen verbinden, gerade „abwesende“ Netze manuell hinzufügen oder auch entfernen. Spezielle Einstellungen pro Netzwerk sind, abgesehen vom ggf. benötigten Zugangsschlüssel, hier in der Regel nicht möglich.

Die Bluetooth-Einstellungen erlauben die Konfiguration der Sichtbarkeit des eigenen Gerätes, die Vergabe eines Gerätenamens sowie das Scannen nach in Reichweite befindlichen sichtbaren Geräten – natürlich nur, wenn Bluetooth auch aktiviert ist.

Über die **VPN**-Einstellungen lassen sich die entsprechenden sicheren Verbindungen ins Firmen-, Uni- oder heimische Netzwerk erstellen und verwalten.

Zu guter Letzt lassen sich über den (im Screenshot nicht mehr sichtbaren) letzten Punkt *Mobilnetze* die Zugangspunkte (**APN**) für das mobile Netzwerk verwalten.

Anrufeinstellungen

Nomen est omen: Hier geht es um unsere Anrufe. Es lassen sich unter *Anrufbegrenzung* zugelassene Rufnummern verwalten und Einstellungen für die zu verwendende Mailbox (im Normalbetrieb sowie im Roaming separat) treffen. Man kann festlegen, ob bei abgehenden Gesprächen die eigene Nummer angezeigt werden soll, ein Profil für die Sprachqualität wählen, die Betreiberauswahl konfigurieren (automatisch aus verfügbaren Netzen auswählen oder einen Betreiber fest einstellen). Auch um eventuelle Anrufweiterleitungen (ständig / bei besetzt / bei nicht antworten / bei nicht erreichbar) lassen sich hier einrichten bzw. verwalten. Dazu gehört übrigens auch, ob und wann die Mailbox „rangingen“ soll. Zu guter Letzt wäre da noch die Sache mit den „Anklopfen“, die sich meist hinter dem Punkt *Zusätzliche Einstellungen* verbirgt.



Bild 2.20: Android-Systemeinstellungen: *Anrufeinstellungen*

Wer nun genau hinschaut, sieht: Mit dem Screenshot habe ich ein wenig gemogelt, der stammt schon von Android 2.3 (aka *Gingerbread*). Das kann man einfach an einem zusätzlichen Konfigurations-Block erkennen: *Einstellungen für Internetanrufe*. Ab Gingerbread ist nämlich von Haus aus die Möglichkeit gegeben, mittels sogenannter *SIP*-Konten Telefonate über das Internet zu führen. Nachdem sich viele Netzanbieter dagegen gesperrt haben, bieten einige davon mittlerweile selbst entsprechende Dienste an. Zu den bekanntesten SIP-Anbietern zählen u. a. SIPGate, 1&1, Dus.NET und QSC.

Töne

Ich höre schon die Beschwerden: „Das sieht bei mir aber ganz anders aus!“ Wahrscheinlich war das bereits bei mindestens einem der vorigen Screenshots so und wird auch bei weiteren wieder auftreten. Das liegt daran, dass jeder Hersteller ein wenig sein eigenes Süppchen kocht und verschiedene Dinge anders einsortiert oder erfreulicherweise zusätzliche Dinge zur Verfügung stellt. Beschränken wir uns also auf Prinzipielles und ignorieren Abweichungen gutmütig.

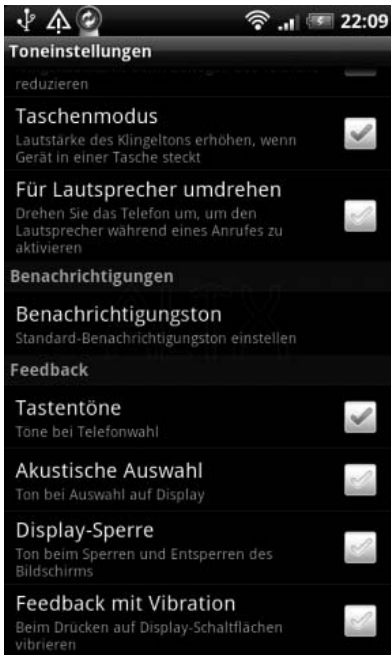


Bild 2.21: Android-Systemeinstellungen: *Toneinstellungen*

Bei den *Toneinstellungen* geht es im Großen und Ganzen also um das, was es auf die Ohren gibt. Separat lassen sich hier die verschiedenen Lautstärke-Einstellungen (Klingelton bei eingehenden Anrufen, Benachrichtigungen, Medien, Wecker...) vornehmen oder das Telefon auch einfach „stumm“ schalten. Der zu verwendende Sound bei eingehenden Anrufen lässt sich auswählen, man kann das „haptische Feedback“ (Vibrieren bei Betätigung von „Soft-Keys“) sowie die Tastentöne bei der Telefonwahl einstellen und mehr (oder auch nicht, je nach Hersteller). HTC bietet beispielsweise noch einen Taschenmodus (siehe Screenshot) – nicht für Billard, sondern für lauterer Klingeln, sollte sich der Androide in einer Tasche befinden (und dies auch bemerken). Motorola hat dafür einen Taschenmodus im *Display*-Menü (siehe nächster Punkt), um selbiges beim Einstecken in die Hosentasche automatisch zu deaktivieren.

Display

Unter *Anzeige* (oder *Display*) finden sich die Einstellungen, die für den Bildschirm relevant sind – wie beispielsweise die Helligkeit, ob die Anzeige automatisch mit ins Querformat gedreht werden soll, wenn das Gerät gedreht wird, und ob Fenster-Animationen angezeigt werden sollen. Ebenso in diesem Menü ist das *Display-Timeout* – also der Zeitraum, nach dem der Bildschirm automatisch abgeschaltet werden soll (sofern der Benutzer „nichts gemacht“ hat).

Weiteres variiert wieder nach Hersteller, und verschiedene *Custom-ROMs* ergänzen auch gern das eine oder andere: Motorola möchte (zumindest beim Milestone 2) automatisch erkennen, ob sich das Gerät gerade in einer Tasche befindet (und bietet für diesen Fall die Option einer automatischen Bildschirm-Abschaltung – funktioniert aber in meiner Hemdtasche schon Mal nicht). Dann gibt es Hersteller, die durch eine automatische Anpassung der Bildschirm-Helligkeit Akku sparen wollen, und anderes mehr.

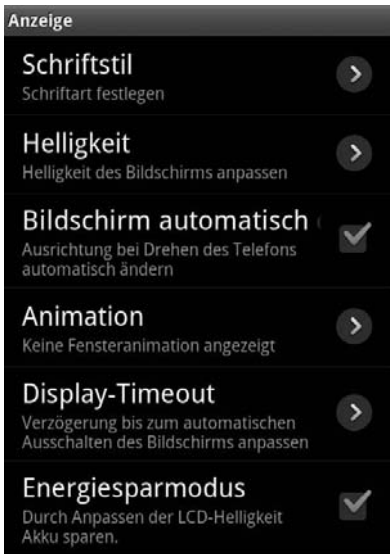


Bild 2.22: Android-Systemeinstellungen: *Display*

Standort und Sicherheit

Wer meint, hier ginge es um Standort *und* Sicherheit, der irrt. Richtig heißen muss es: Standort *oder* Sicherheit. Spätestens ab Android 2.3 (Gingerbread) gibt es nämlich nur noch eins von beidem: Wer die (energiesparendere) Standortbestimmung über Mobilfunkmasten und WLAN-Netzwerke nutzen möchte, muss Google seine Standortdaten zur Verfügung stellen – ein Opt-Out bei gleichzeitiger Nutzung des Services ist nicht (mehr) vorgesehen (wie sich das dennoch bewerkstelligen lässt, findet sich im Abschnitt 1.2 beim Thema *Location-Cache*).

Daneben (oder der Anordnung nach besser „darunter“) gibt es natürlich die Möglichkeit, die Standort-Bestimmung über **GPS** ein- bzw. auszuschalten. Sofern die andere Ortsbestimmungsart nicht aktiviert wurde, sammelt hier (hoffentlich?) keiner Daten mit. Und solange nicht tatsächlich eine Ortsbestimmung durchgeführt wird, kostet das auch nicht wirklich Energie. Wenn aber doch, dann gleich richtig: Da kann es durchaus passieren, dass nach ca. vier Stunden Navigation der Akku aufgibt.



Bild 2.23: Android-Systemeinstellungen: **Standort und Sicherheit**

Passend zum Thema lässt sich bei manchen Geräten in diesem Menü auch der Kompass kalibrieren. Auch das Thema „Sicherheit“ ist gelegentlich an diesem Ort untergebracht: Display-Sperre, SIM-Sperre, Geräteverwaltung (Einrichten/Verwalten von Geräteadministratoren) sowie Zertifikate lassen sich zumindest auf dem *Motorola Milestone 2* in diesem Menü finden.

Konten

Hier fällt die Länge der Liste zum Teil sehr unterschiedlich aus, was zum einen mit dem Hersteller und seiner „Zwangsbeglückung“ zu tun haben kann (siehe „Aktien“ im Screenshot eines HTC-Gerätes), zum anderen aber nicht zuletzt davon abhängt, wie viele „Konten“

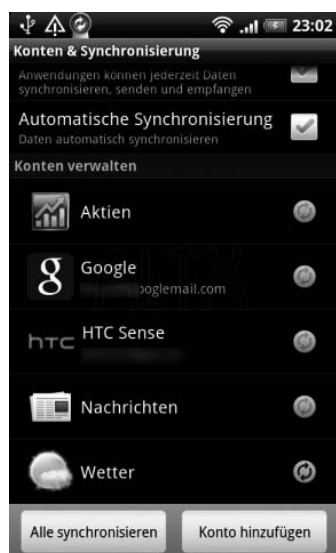


Bild 2.24: Android-Systemeinstellungen: **Konten und Synchronisierung**

(z. B. Google-Accounts) man eingebunden hat. Natürlich spielt es auch eine Rolle, ob der Hersteller einen Geräte-Spion (HTC: Sense.COM, Motorola: Blur etc.) zur Auffindung eines „verlorenen“ Gerätes integriert, der Anwender ihn eingerichtet hat und nutzt (im Screenshot: „HTC Sense“).

Nach Auswahl des Google-Kontos ließe sich hier auch konfigurieren, ob Kontakte und Kalender automatisch synchronisiert werden sollen. Gut versteckt – und natürlich per Default aktiviert. Das „zentrale Häkchen“ für die automatische Synchronisation, wie auf dem Screenshot zu sehen, fehlt beispielsweise bei oben genanntem *Motorola Milestone 2* ebenso wie die Möglichkeit, die Hintergrund-Synchronisation zu deaktivieren (beide „Häkchen“ sind bei HTC-Geräten vorhanden) – auch an anderer Stelle konnte ich sie bislang nicht finden. Wie gut, dass es für so etwas *Schnellumschalter* (vgl. Abschnitt 2.4) gibt.

Anwendungen

Anwendungen konfigurieren? Nein, vielmehr geht es um deren Verwaltung. Werden beispielsweise die *unbekannten Quellen* nicht aktiviert, ist eine Installation nur über den Playstore möglich – um also eine App aus einer vom Entwickler zur Verfügung gestellten APK-Datei installieren zu können, muss das Häkchen hier zwingend gesetzt werden.

Unter *Anwendungen verwalten* werden alle installierten Apps aufgelistet. So kann man hier nachschauen, wie viel Platz die Apps selbst belegen, wie viele Daten sie verwalten und wie groß der vorgehaltene Cache gerade ist. Und man kann all diese Dinge auf einen Schlag oder auch einzeln löschen – wobei das Löschen einer App auch automatisch das Löschen ihrer Daten und ihres Caches nach sich zieht, nicht aber umgekehrt. Dies ist beim Playstore manchmal ganz hilfreich, wenn der sich gerade wieder verhaspelt hat: Cache löschen, neu initialisieren lassen.

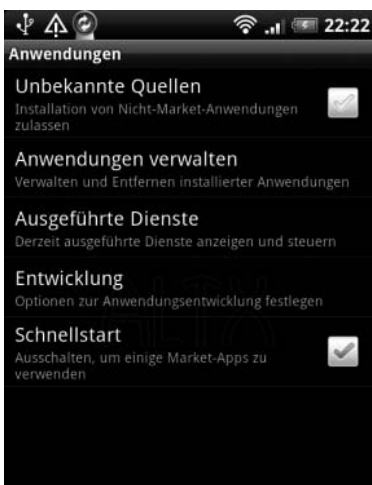


Bild 2.25: Android-Systemeinstellungen: *Anwendungen*

Hinter den *Ausgeführten Diensten* verbirgt sich ein Mini-Task-Manager. Dieser zeigt u. a. an, welche Apps gerade ausgeführt werden, seit wann, und wie viel Speicher sie belegen, Letzteres sowohl einzeln als auch in Summe. Ebenfalls an dieser Stelle zu sehen: welche Apps welche Services gestartet haben. Der bekannteste Übeltäter dürfte Google Maps mit seinem *NetworkLocationService* sein – läuft ständig, auch wenn man Maps nie genutzt hat (wird vermutlich für die netzbasierte Standortbestimmung genutzt, doch sicher sagen kann das scheinbar niemand). Durch Antippen eines Eintrags erhält man die Möglichkeit, einen Dienst anzuhalten – oder auch nicht. Das „oder auch nicht“ bezieht sich zum einen auf die Möglichkeit, diese Aktion abzubrechen, zum anderen aber auch auf den Fakt, dass die meisten Dienste ohnehin nach wenigen Sekunden wieder gestartet sind (worauf der Dialog auch hinweist).

Dann wäre da noch der Punkt *Entwicklung* – nicht nur für Entwickler. Hier verstecken sich auch Dinge wie „Display aktiv lassen, wenn Ladekabel angeschlossen“.

Weitere Punkte sind wiederum Hersteller- und Geräte-abhängig, wie etwa der *Schnellstart* bei neueren HTC-Geräten oder die Frage, was bei „2x Home“ gestartet werden soll (Milestone 2).

Datenschutz

Schon wieder etwas Doppeldeutiges: Möchte Google hier unsere Daten schützen (indem es sie auf seine Server sichert) oder sollen wir hier unsere Daten vor Google schützen, indem wir alle Häkchen entfernen? Sollte letztere Variante die richtige sein, ist die Umsetzung nur teilweise gelungen, denn K&K (Kalender und Kontakte) ignorieren diese Einstellung geflissentlich und synchronisieren trotzdem.



Bild 2.26: Android-Systemeinstellungen:
Datenschutz

Scherz beiseite: Gemeint ist, dass die eigenen Einstellungen sowie Anwendungsdaten auf die Server von *Google Inc.* gesichert werden bzw. nach einem Werksreset von dort wieder hergestellt werden sollten. Warum der Konjunktiv an dieser Stelle? Dieser Service funktioniert leider nicht immer so zuverlässig, wie man es sich wünschen würde. So liest man im **Bug-Tracker** von etlichen Fällen, in denen Apps und Daten nur teilweise oder überhaupt nicht wieder hergestellt wurden.



<http://code.google.com/p/android/issues/detail?id=17354>

Und was wird hier überhaupt gesichert? Für Geräte, auf denen Android 3.x oder höher eingesetzt wird, handelt es sich etwa um folgende Daten:

- Android-Einstellungen wie WLAN-Netzwerke mit ihren Passwörtern, das Benutzer-Wörterbuch etc.
- Einstellungen vieler Google-Apps, einschließlich der Lesezeichen des Web-Browsers
- die aus dem Playstore installierten Apps
- Daten von anderen Apps, sofern die Entwickler dies explizit implementiert haben

Es handelt sich hierbei also mitnichten um ein vollständiges Backup: Daten von Apps werden nur dann mitgesichert, wenn diese Apps das auch explizit unterstützen – was für viele Apps nicht zutreffen dürfte. Und natürlich sind auch die auf der SD-Karte abgelegten Dateien nicht in diesem Backup enthalten. Das bedeutet, dass man sich zumindest nicht auf dieses Backup allein stützen sollte. Auch ist es nicht jedermanns Ding, seine Daten einer Cloud anzuvertrauen – auch wenn dies (Achtung!) die Voreinstellung ist.

Der Werksreset ist übrigens ein weiterer Punkt, der sich auf vielen Geräten in diesem Menü findet: „Zurücksetzen auf Werkseinstellungen“, entweder für den Fall, dass gar nichts mehr geht, oder wenn man das fragliche Gerät veräußern möchte, denn bei einem „Werksreset“ werden alle Anwenderdaten einschließlich der vom Anwender installierten Apps gelöscht. Lediglich die eventuell vorhandene SD-Karte bleibt dabei völlig unberührt (abgesehen von *App2SD*).

SD-Karte und Telefonspeicher

Wenn jemand seinen Speicherplatz sucht: Hier wird er fündig. Dass der Inhalt auf dem Screenshot so umfangreich ist, liegt am Gerät: Das *Samsung Galaxy S* hat zusätzlich zu „Telefonspeicher“ und „externer SD-Karte“ auch noch eine „interne SD-Karte“ (richtiger gesagt: Die „interne Karte“ wurde in „Telefonspeicher“ und „interne SD-Karte“ aufgeteilt – von SD-Karten mit 6 Gigabyte Speicher habe zumindest ich noch nichts gehört oder gelesen; nimmt man jedoch den Telefonspeicher dazu, kommt man auf vertraute 8 Gigabyte.).

Hier findet man heraus, wie viel Speicher insgesamt vorhanden und wie viel davon verfügbar ist – sowohl auf Karten als auch im Telefonspeicher. Darüber hinaus lässt sich die

SD-Karte aus diesem Menü heraus formatieren oder auch „deinstallieren“ (unter Windows heißt das „sicher entfernen“; gemeint ist also, dass das System auf die physikalische Entfernung aka Entnahme der SD-Karte vorbereitet wird).



Bild 2.27: Android-Systemeinstellungen: **SD-Karte und Telefonspeicher**

Sprache und Tastatur



Remote Web
Desktop

In diesem Menü geht es um die Lokalisierung. Das betrifft zum einen Spracheinstellungen, nach denen sich auch die Apps (sofern entsprechend angepasst) richten sollen – damit man auch versteht, was man da liest. Durch das zugehörige Land werden darüber hinaus auch Dinge wie das Datums- und Uhrzeitformat sowie das zu verwendende Einheiten-System (metrisch oder imperial) beeinflusst.

Zum zweiten geht es aber auch um die zu verwendende Tastatur („Eingabe-Methode“) und deren Konfiguration. Wie am Screenshot erkennbar, ist beim *Milestone 2* die Tastatur-App *Swype* vorinstalliert und lässt sich daher hier auch konfigurieren, und zwar inklusive der von ihr unterstützten Sprachen, die sich im laufenden Betrieb so dann durch ein Wischen über die Leertaste wechseln lassen. Die im Screenshot angezeigte Option *WiFi Keyboard* hingegen ist nicht von Haus aus dabei: Hier handelt es sich um eine Ergänzung der App *Remote Web Desktop*. Aktiviert man diese, kann man die PC-Tastatur verwenden, um Texte am Androiden zu erfassen. Unter *Tastatur des Gerätes* wiederum ist die Hardware-Tastatur des *Milestone 2* zu verstehen.



Bild 2.28: Android-Systemeinstellungen: *Sprache und Tastatur*

Der letzte Punkt ist das *Nutzerwörterbuch*, das die selbst hinzugefügten Begriffe für die automatische Worterkennung enthält. Hier lassen sich neue Wörter direkt hinzufügen, aber auch eventuell falsch/versehentlich erfasste Wörter wieder entfernen.

Spracheingabe/-ausgabe

Dem Screenshot nach ein kurzes Menü, doch hinter den beiden dargestellten Punkten verbirgt sich eine wahre Flut an Einstellungen. Der erste Punkt bedenkt die *Google-Spracherkennung*: Welche Sprache wird gesprochen? Mit welchen Einstellungen soll die Suchoption *SafeSearch* versehen werden? Sollen Beleidigungen automatisch gesperrt, sollen im Suchfeld Hinweise eingeblendet werden?

Ähnlich sieht es für die Sprachausgabe, auch TTS (Text-To-Speech) genannt, aus. Für diese lassen sich Sprache, Stimme, Sprechgeschwindigkeit, Sprachmodul und gegebenenfalls auch Sprachdaten konfigurieren bzw. installieren.

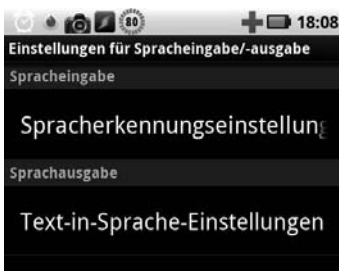


Bild 2.29: Android-Systemeinstellungen: *Spracheingabe/-ausgabe*

Eingabehilfen

Was zum Geier sind denn nun Eingabehilfen – Tastatur und Spracheingabe hatten wir doch schon? Derartige „Eingabehilfen“ sind hier auch nicht gemeint; dieser Punkt richtet sich vielmehr an Menschen mit Behinderungen. Da wäre zuerst die *Sprachwiedergabe*: Hat der Benutzer so schlechte Augen, dass er zwar den Text sieht, ihn aber nicht lesen kann, kann er ihn sich durch „Antippen“ vorlesen lassen. Ähnlich verhält es sich mit dem *Zoom-Modus* zur Vergrößerung von Elementen.

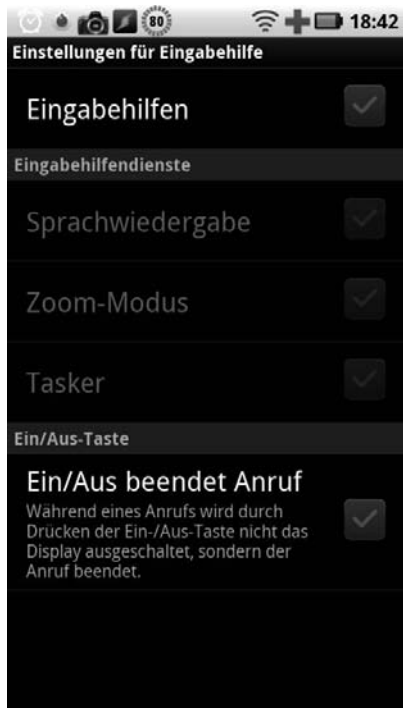


Bild 2.30: Android-Systemeinstellungen:
Eingabehilfen

Dass *Tasker* hier auftaucht, hat eine andere Bewandnis: Er braucht die entsprechenden Berechtigungen, um im „Benutzer-Interface“ (also auf dem Bildschirm) dargestellte Elemente auswerten zu können.

Einfach und verständlich hingegen ist der letzte dargestellte Punkt: *Ein/Aus beendet Anruf*. Gut für alle die, die den entsprechenden Button auf dem Bildschirm nicht finden können: Statt das Display auszuschalten, wird dann per Ein/Aus-Taste ein laufendes Gespräch beendet, natürlich nur, wenn eines läuft. Das hat bei manchen den dummen Nebeneffekt, dass sie mitten im Telefonat versehentlich auflegen – weil sie zum „Eben-mal-etwas-Nachschauen“ das Display anschalten wollen.

Datum und Uhrzeit

Dieses Menü sollte einfach und verständlich sein – eigentlich erübrigt sich hier fast jede Erklärung. Hier lässt sich bei Bedarf die Zeit manuell korrigieren, falls das Netzwerk des Betreibers das nicht hinbekommt. Normalerweise sollte dies recht selten bis nie nötig werden. Einzig die Umschaltung vom 12- auf den 24-Stunden-Modus (oder umgekehrt) sowie die Anpassung des Datumsformates kann, je nach Vorliebe, für den einen oder die andere interessant werden.



Bild 2.31: Android-Systemeinstellungen: *Datum und Uhrzeit*

Telefoninfo

Das letzte Menü birgt eine Menge Potenzial. Zuerst finden sich hier die vom Betreiber bereitgestellten Systemsoftware-Updates – für all die Ungeduldigen, die nicht auf die entsprechende automatische Benachrichtigung warten können oder wollen. Dies ist der einzige Punkt, in dem auch eine Aktivität ausgelöst wird: das Einspielen eines Updates, so denn eines gefunden wird.

Alle anderen Punkte spucken hingegen jede Menge nützlicher Informationen aus – und sind auf verschiedenen Geräten unterschiedlich zusammengefasst. Sie informieren über Akkustatus (Laden/Entladen) und -stand, die eigene Telefonnummer, das aktive Netzwerk (Provider) sowie dessen Signalstärke und Typ, Roaming, Mobilnetzstatus, IMEI, MAC-Adressen und Betriebszeit und geben schließlich diverse Informationen zum verwendeten System.



Bild 2.32: Android-Systemeinstellungen: *Telefoninfo*

Unter dem Punkt *Akku* (der beispielsweise auf dem *Motorola Milestone 2* komplett aus diesem Menü genommen und in ein eigenes verfrachtet wurde) findet man in der Regel auch eine Liste der größten Verbraucher. Diese scheint nach meinem Eindruck jedoch mit fortschreitender Android-Version immer „allgemeiner“ zu werden – vielleicht täusche ich mich da aber auch.

Denn mit Gingerbread kam zumindest ein neues Feature hinzu: die abgebildeten Statistiken zum Batterieverbrauch. Zu diesen gelangt man, wenn man im Menü *Akku* auf den „Balken“ am oberen Bildschirmrand tippt – der sich bei genauerem Hinschauen als Mini-Graph entpuppt, wie der „große Graph“ auf dem Screenshot deutlich macht.

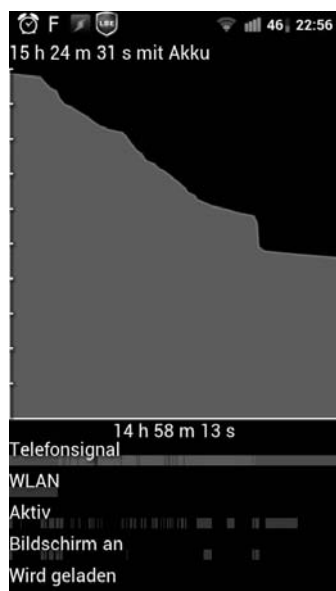


Bild 2.33: Android-Systemeinstellungen: *Akku-Verbrauchs-Informationen*

Während dieser „große Graph“ veranschaulicht, wie (un)gleichmäßig der Akku entladen wurde, finden sich unmittelbar darunter einige wertvolle Details, beispielsweise zum Telefonsignal: Ein sattes Grün steht für eine sehr gute Signalstärke; wird es heller, war das Signal schwach. Kritisch wird es bei roten Stellen: Hier war gar kein Signal vorhanden – das Smartphone hat aber mit aller Gewalt versucht, eines zu finden. Im Luftschutzbunker relativ sinnlos! Wenn es kein Signal gibt (etwa aufgrund starker Stahlbeton-Wände oder weil man sich etwa irgendwo abseits jeglicher Zivilisation befindet), bedeutet dies nur eins: Hoher Akku-Verbrauch, da das Gerät mit voller Leistung auf (nutzlose) Suche geht. Tritt dies jeden Tag zur gleichen Zeit auf, sollte man die zugehörige Örtlichkeit prüfen – und ggf. per *Automat* hier in den Flugzeugmodus wechseln.

Die übrigen vier Graphen sind eigentlich selbsterklärend: Wann war WLAN aktiviert, wann das Gerät beschäftigt, wann der Bildschirm eingeschaltet und wann das Ladekabel angeschlossen (natürlich beidseitig)?

Ausgewählte bzw. häufig genutzte Einstellungen

Schnell und ohne große Umstände an die wichtigsten Einstellungen gelangen – darum geht es hier. Wenn ein pures Umschalten im Sinne von „An/Aus“ gefragt ist, haben wir dieses Thema ja bereits bei den **Schnellumschaltern** abgehandelt. Doch nicht alles ist dort enthalten. Daher schauen wir nach, was es noch so gibt.

„Schnelle Einstellungen“ – auf Englisch hieße das „Quick Settings“. Und mindestens vier Apps tragen genau diesen Namen. Die bestbewertete App davon ist **Quick Settings** von Sergej Shafarenka: durchschnittlich 4,7 Sterne bei fast 35.000 Bewertungen sind schon allerhand! Die App verankert sich, wie im Screenshot (Bild 2.34) ersichtlich, mit einem Symbol in der Statuszeile. Von dort gelangt man in das dargestellte Menü und findet die wichtigsten Schalterchen vor. Über den kleinen Knopf neben „Ringer“ erreicht man eine Reihe von Schieberreglern für die verschiedenen Lautstärken (Klingelton, Benachrichtigung, Medien etc.).



Quick Settings
(Sergej Shafarenka)



Bild 2.34: *Quick Settings* ermöglicht einen Schnell-Zugriff auf häufig benötigte Einstellungen



Quick Settings von
APS



<http://www.androidpit.de/de/android/forum/thread/422713/>

Zwei Gimmicks sind auch noch zu erkennen: Die Taschenlampen-Funktion und, etwas versteckt, die Liste der Stromverbraucher. Letztere öffnet sich, wenn man das Batterie-Symbol antippt.

Gleicher Name, andere App: **Quick Settings** von APS (Bild 2.35). Auch hier ein recht ähnliches Popup, auf welches man auf verschiedene Art zugreifen kann: über die Statusleiste, langes Drücken auf die „Such“-Taste oder langes Drücken auf die Kamera-Taste, wie man es eben konfiguriert hat. Neben einer ganzen Reihe von Schnellumschaltern finden sich auch bei dieser App die Schieberegler für die Lautstärke. Als praktisches Extra gibt es eine Übersicht über wichtige Systemdaten: Genauer Akkustand, Anzahl installierter Apps sowie gesamter und verfügbarer Speicher (intern und SD-Karte).

Da die anderen mir bekannten „Schnelleinsteller“ ähnlich aufgebaut sind, möchte ich sie nicht alle einzeln vorstellen. Stattdessen kann sie jeder bei Bedarf in *der Übersicht* bei AndroidPIT selbst nachschlagen.



Bild 2.35: Ein weiteres **Quick Settings** mit Schnellzugriff auf wichtige Details

Zusätzliche bzw. versteckte Einstellungen

Wenn es um zusätzliche Konfigurationsmöglichkeiten geht, die das System von sich aus in der Form nicht anbietet, fällt den meisten sicher als erstes *Spare Parts* ein oder besser noch, da aktueller und ohne Werbung: *Spare Parts Plus*. Diese App stellt nicht nur einzelne zusätzliche Einstellungen zur Verfügung, die nicht selten wesentlich mehr ins Detail gehen als die Bordmittel (beispielsweise Animationen, siehe Screenshot: nicht nur ein simples globales „An/Aus“, sondern explizite Einzelheiten). Manche Anwender werden sich zudem über die Möglichkeit freuen, die Größe der Systemschrift anpassen zu können. Und darüber hinaus versorgt uns *Spare Parts Plus* auch noch mit etlichen detaillierten System-Statistiken, wie ebenfalls auf dem Screenshot erkennbar.



Spare Parts Plus

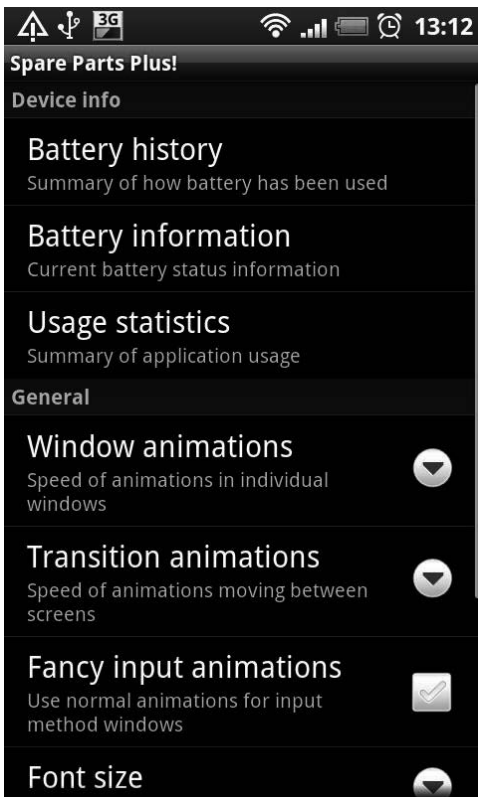


Bild 2.36: *Spare Parts Plus!* bietet Zugriff auf zusätzliche Einstellungen

Die App ist so gut, dass sich das Team des bekannten *Custom-ROMs CyanogenMod* entschlossen hat, es von vornherein in sein ROM einzubauen. Und wenn die App gut gefällt, der kann für knapp anderthalb Euro auch zur Pro-Version greifen.



Blade Buddy

Wer seinen Androiden mit **root**-Rechten ausgestattet hat, greift vielleicht eher zu **Blade Buddy** (Bild 2.37) oder dessen Pro-Version, beide aus demselben Hause wie *Spare Parts*. Die App integriert sich in *Spare Parts* (bzw. lässt sich aus selbigem heraus aufrufen) und erlaubt die Konfiguration etlicher systeminterner Schalterchen.

Der Screenshot gibt einen ganz groben Überblick über die bereitgestellten Funktionalitäten. So lässt sich das Auslösegeräusch der Kamera abschalten, die Dalvik-VM detailliert anpassen, oder auch die Boot-Animation deaktivieren. Aktionen wie ein schneller Reboot oder das beschreibbare Einhängen der Systempartition stellen die App ebenfalls vor keinerlei Probleme.

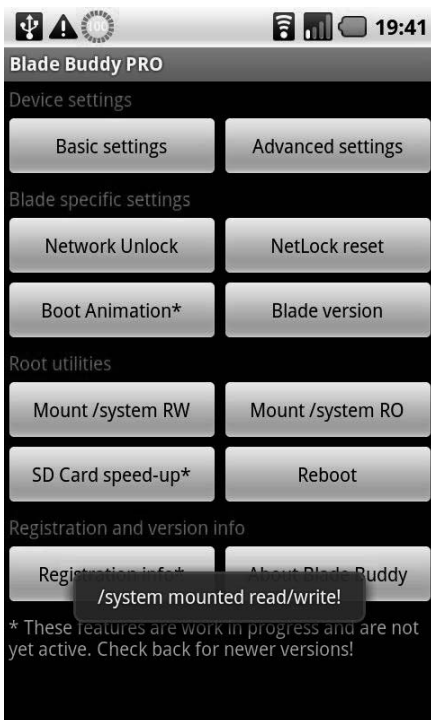


Bild 2.37: *Blade Buddy* integriert sich in *Spare Parts* und legt weitere Schalterchen frei

Natürlich wird vor all zu wildem „Gespiele“ gewarnt. Einige dieser Einstellungen hat Google nicht umsonst vor dem „Otto Normalanwender“ versteckt und für Nicht-Rootler unzugänglich gemacht: Das falsche Schraubchen zu weit gedreht, und da fliegt das Blech weg. Man kann sich sein System auch kaputt konfigurieren – also bitte mit Bedacht vorgehen!

Aber benötigt man zum Sichtbarmachen „versteckter“ Einstellungen nun wirklich immer extra Apps? Oder gibt es auch andere Möglichkeiten, daran zu gelangen? In der Tat gibt

es für so manche „Secret Settings“ auch passende „**Secret Codes**“ – wie beispielsweise `*#*#4636#*#*`. Diese gibt man so ein, als wollte man bei der entsprechenden Nummer anrufen. Und in diesem Beispiel öffnet sich dann ein recht informatives Menü, welches auch *Spare Parts* und **Secret Phone Settings** (Bild 2.38) nutzen. Wobei bei letzterer App das dauernde „Info“ auf den Buttons leicht irritiert: Ja, es werden etliche hilfreiche Informationen angezeigt, dabei lässt sich aber durchaus auch die eine oder andere Einstellung anpassen (siehe Screenshots auf der Playstore-Seite).



Secret Phone
Settings



Bild 2.38: *Secret Phone Settings* legt versteckte Einstellungen frei

Neben diesen Tools für vielfältige allgemeine Einstellungen gibt es auch noch einige, die sich auf Einzelbereiche spezialisiert haben. So lassen sich etwa mit dem **WiFi Advanced Config Editor** für jedes konfigurierte WLAN erweiterte Einstellungen wie der Index des WEP-Schlüssels oder WPA Enterprise Parameter (z. B. `wpa_supplicant`) anpassen, mit **Set DNS** zu verwendende NameServer und andere **DNS**-Parameter konfigurieren und (**root**-Rechte vorausgesetzt) sogar mit **ProxyDroid** die Verwendung eines **Proxy-Servers** (auch abhängig von der Verbindungsart: mobil oder WLAN) erzwingen.



WiFi Advanced
Config Editor



Set DNS



ProxyDroid

Nicht ganz uninteressant wäre auch die Möglichkeit, die Synchronisation von Kalender, Kontakten, Google Mail & Co. auf die Zeiten zu beschränken, zu denen man mit einem WLAN und/oder einer Stromquelle verbunden ist – **SmartSync** macht dies möglich. Root-Usern vorbehalten bleiben allerdings Dinge wie die Anpassung der CPU-Taktung (das bekannteste Tool hierfür wäre sicherlich **SetCPU**, aber auch der **CPU-tuner** ist definitiv einen Blick wert!) oder die Bildschirm-Auflösung (z. B. mittels **LCDDensity**).



SmartSync



SetCPU



CPU-tuner



LCDDensity

Und wer jetzt noch mehr Möglichkeiten oder Alternativen sucht, wird in der Übersicht bei AndroidPIT fündig.



<http://www.androidpit.de/de/android/forum/thread/422713/>

2.5 Automatisierung

Einstellungen sind ja gut und schön. Einmal gemacht, merkt sie sich unser Android auch brav. Aber passen sie auch zu jeder Gelegenheit? Tagsüber auf der Baustelle muss ein eingehender Anruf möglichst laut signalisiert werden, damit man ihn auch mitbekommt. Doch wer lässt sich schon gern nach Feierabend von lautem Handyklingeln aufschrecken?

Und das ist erst der Anfang: Das Umschalten zwischen verschiedenen Klingeltönen und Lautstärken vergessen wir ebenso leicht wie das Aktivieren von GPS vor dem Start der Kartensoftware – oder das Hochschrauben des Display-Timeouts vor Aktivierung des RSS- bzw. eBook-Readers.

Für all diese Dinge muss es doch auch Helferlein geben? Wir sind doch sicher nicht die Ersten, die vor diesem Problem stehen! Das ist beides korrekt. Und so gibt es Apps, die uns gewisse Dinge abnehmen können: zeitgesteuert, abhängig vom aktuellen Standort („location-based“ oder „ortsbasiert“ genannt) oder auch kombiniert bzw. bei anderen Events. Und es gibt *Tasker*. Der passt in keine dieser Kategorien: *Tasker* ist eher ein

„Wundertool“, „Schweizer Offiziersmesser“ oder einfach das Ultimate Werkzeug (Englisch: „TUT“, The Ultimate Tool), man braucht aber als Einsteiger auch mindestens ein „Tut“ (Tutorial) – doch dazu später...

Ein Tipp noch vorweg: Automatisierungs-Tools (die übrigens in einer Übersicht bei AndroidPIT zusammengefasst sind) sollten möglichst nicht auf der SD-Karte installiert werden. Sonst werden sie beendet, wenn man seinen Androiden per USB mit dem Computer verbindet.



<http://www.androidpit.de/de/android/forum/thread/423710/>

Zeitschaltuhren

Geht es um reines zeitbasiertes Schalten, ist **Timeriffic** (Bild 2.39) nicht nur das bekannteste, sondern auch das am besten bewertete Tool. Ein Großteil der oben genannten Aufgaben lässt sich damit erledigen: Lautstärken, Stummschaltung, Vibrator. Auch Flugzeugmodus, WLAN und Bluetooth beherrscht die App. All diese Dinge lassen sich zu beliebigen Zeitpunkten auf beliebige Werte stellen – was übrigens auch für die Bildschirm-Helligkeit gilt.



Timeriffic



Bild 2.39: *Timeriffic* ist das Cron für Android

Übrigens nicht nur Uhrzeit-basiert: Auch die Wochentage lassen sich dazu auswählen. Der Screenshot zeigt das ganz gut: So lassen sich etwa für das Wochenende andere Regeln erstellen als für werktags.



Android Audio Profile

Das war es aber auch bereits – mehr ist nicht drin. **Android Audio Profile** bietet etwa das Gleiche an (mit der zusätzlichen Möglichkeit, eine Schaltung per Widget vornehmen zu können). Und damit ist dann – für die reinen Zeitschaltuhren – auch schon das Ende der Fahnenstange erreicht.

Ortsbasiertes Schalten



Location Profile

Hier gibt es eigentlich nur zwei Kandidaten: Das auf die übrigen klassischen Profile beschränkte **Location Profile**, welches sich lediglich um Lautstärke, Klingeltöne, Vibration sowie Hintergrundbilder („Wallpaper“) kümmert – und **Llama** (Bild 2.40).

Llama gibt sich vielfältiger. Abhängig von den jeweiligen Standorten (der Reiter *Areas* im Screenshot), kann sich die App neben den genannten klassischen Audio-Profilen auch um Dinge wie **APNs**, Hintergrundbilder, WLAN und den Flugzeugmodus kümmern oder den Androiden neu starten, Apps starten/beenden und mehr. Mittlerweile lassen sich auch andere Events zum Schalten heranziehen: Angeschlossene Ladekabel, Docking-Stationen, Kalender-Ereignisse, in der Nähe befindliche Bluetooth-Geräte ...



Llama

Bild 2.40: **Llama** ermöglicht nicht nur ortsabhängiges Schalten

Damit zieht die App fast mit *Locale* (siehe unten) gleichauf – nur dass es kein GPS benutzt und die entsprechenden Plugins nicht unterstützt.

Zeit-, Orts- und eventbasiertes Schalten

Der Name verrät bereits, was sich mit **Phone Profiles** schalten lässt: die klassischen Telefon-Profil-Eigenschaften. Hinzu kommen noch WLAN, Bluetooth, der Flugzeugmodus sowie Bildschirm-Helligkeit und Ausrichtungsmodus. Ortsbasiertes Schalten unterstützt die App zwar nicht – dafür aber neben zeitbasiertem Schalten eine ganze Reihe Events: etwa ein angeschlossenes Ladekabel oder einen bestimmten Akkustand. Damit lassen sich energiehungrige Aktionen einschränken – wobei ich beispielsweise an ein Dimmen des Displays oder an das Abschalten der WLAN-Funktionalität bei niedrigem Akkustand denke.



Phone Profiles

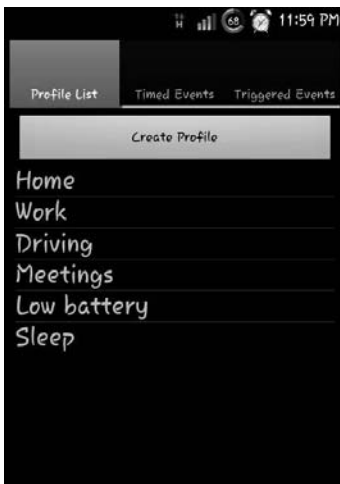


Bild 2.41: *Phone Profiles* kümmert sich um die klassischen Telefon-Profile

Mindestens genauso praktisch ist das Schalten anhand bestimmter Kalendereinträge: Bei Sitzungen klingelt es nicht mehr, und auch beim Theaterbesuch ist es ruhig. Leider lässt sich derzeit wenig zur Zuverlässigkeit von *Phone Profiles* sagen, es gibt im Playstore noch keine aussagekräftigen Kommentare.

Das sieht bei **EasyProfiles** (Bild 2.42) ganz anders aus: Sowohl im Google Playstore als auch bei AndroidPIT finden sich zahlreiche, überwiegend positive Bewertungen einschließlich Kommentaren. Es scheint mir recht eindeutig: Diese App hat dem einstmaligen Spitzenreiter *Locale* den Rang abgelassen. Sogar die zahlreichen *Locale*-Plugins werden hier unterstützt, und *EasyProfiles* selbst kostet bei vergleichbarem Leistungsumfang mit ca. dreieinhalb Euro gerade einmal die Hälfte!



Bild 2.42: *EasyProfiles* ist ein Allrounder, der **Locale** den Rang abgelaufen hat



EasyProfiles

Hervorragender Support und übersichtliche Bedienung gehen bei *EasyProfiles* mit hoher Flexibilität Hand in Hand. Neben automatischen Aktionen lassen sich Profile sogar manuell aktivieren. Die App ist in der Lage, zahlreiche Konfigurationsänderungen vorzunehmen: alles, was zuvor genanntes *Phone Profiles* schalten kann, und zusätzlich Synchronisations-Einstellungen (AutoSync, Hintergrunddaten), APN, 2G/3G/4G, Display (Helligkeit, Timeout, Wallpaper, AutoRotate) und mehr.

Als Auslöser kommen neben Zeit und Ort auch Dinge wie Kalendereinträge, Akku-Stand, Bluetooth/WLAN-Verbindungen, Dockingstation/Ladekabel und sogar die im Vordergrund befindliche App in Frage. Da sich all dies noch zusätzlich durch Verwendung von Locale-Plugins erweitern lässt, haben wir bei dieser App alle eingangs genannten Szenarien abgedeckt.

Nicht unerwähnt bleiben darf natürlich der Klassiker in dieser Rubrik: Lange Zeit galt **Locale** (Bild 2.43) als die einzige echte Lösung. Und was war davor?

*Judge Robert Restaino **jailed 46 people** when a mobile phone rang in his New York courtroom and no one would admit responsibility. So we invented Locale. Problem solved. (Im Mai 05 hat Richter Restaino 46 Leuten eine Haftstrafe verordnet, da keiner zugeben wollte, dass es sein Telefon war, welches im New Yorker Gerichtssaal klingelte. Da erfanden wir Locale. Problem gelöst.)* So ist es auf der **Website** zu lesen. Vergleichsweise einfach zu erfassen und bedienen, wäre *Locale* auch heute noch im Ranking weiter vorn – gäbe es da nicht das Handicap des Preises: Gut sieben Euro sind im App-Market einfach ein wenig viel, da schaltet so mancher bereits ab, ohne weiter zu lesen.



Bild 2.43: *Locale* ist der Klassiker in dieser Rubrik und wird von zahlreichen Plugins unterstützt

Locale bietet im Prinzip alles, was auch *EasyProfiles* im Portfolio hat. Ob die Bedienung hier intuitiver oder einfach nur vergleichbar ist, muss jeder für sich entscheiden. Ich habe *Locale* eine Zeit lang benutzt und sehe eigentlich nichts, was *EasyProfiles* zum halben Preis nicht bieten würde – abgesehen vielleicht von der längeren Erfahrung, die das *Locale*-Team mitbringen dürfte. Wobei ich nicht sagen kann, ob das geniale Prinzip des „Schichten-Aufbaus“ dort auch übernommen wurde: Bei *Locale* bauen die Profile nämlich aufeinander auf. Das „unterste“ Profil bildet die „Basis“, und die „darüber liegenden“ Profile wenden lediglich davon abweichende Einstellungen an. Wird also „weiter oben“ ein Profil inaktiv, tritt automatisch der aus den „darunter liegenden“ aktiven Profilen bestimmte Zustand ein – wobei die Eigenschaften der „weiter oben liegenden“ jeweils Vorrang haben. So lässt sich jederzeit leicht erkennen, was Sache ist.



Locale

Tasker

Ein eigener Abschnitt für eine einzige App sei ungerechtfertigt? Dem kann ich in sofern zustimmen, als man **Tasker** ein eigenes Buch widmen könnte: „Android-Automation mit Tasker“. *Tasker* ist nicht irgend eine Automatisierungs-App – es ist *die* Automatisierungs-App schlechthin. Ist etwas mit Tasker nicht hinzubekommen, dann geht es schlicht und ergreifend nicht. Auch nicht mit einer anderen App. Selbst im AndroidPIT-Forum findet sich kaum eine Frage, auf die nicht irgend jemand mit „Tasker“ geantwortet hätte.



Tasker

Tasker kann alles das, was auch *Locale* kann, einschließlich der Verwendung der Plugins. Ach was: *Tasker* kann alles, was irgend eine der vorgenannten Apps kann. Und das in beliebiger Kombination. Und mehr. Viel mehr!



Bild 2.44: *Tasker* ist das ultimative Automatisierungs-Werkzeug

Auch bei *Tasker* erstellt man „Profile“. Dargestellt werden diese in der Übersicht etwa so, wie man es auf Bild 2.44 erkennen kann – zweiseitig: Links der (bzw. die) Auslöser („Kontext“ genannt), rechts das, was passieren soll („Tasks“, also Aufgaben). Bereits an diesem einen Screenshot lässt sich erahnen, wie vielfältig *Tasker* einsetzbar ist: Als Auslöser lassen sich neben den bisher besprochenen „gewöhnlichen“ Dingen wie Zeit, Tag und Ort etwa Apps im Vordergrund, Hardware/Software-Status, Ereignisse, Widgets oder Timer einsetzen. Auch der Erhalt einer SMS mit einem bestimmten Text oder der Anruf von einer bestimmten Telefonnummer sind möglich.

Ebenso vielfältig schaut es bei den Möglichkeiten für Tasks aus. Aufgrund ihres Umfangs mussten diese bereits in grauer Vorzeit auf Kategorien verteilt werden (Bild 2.45; die Zahl besagt, wie viele Elemente in einer Kategorie enthalten sind). Außerdem lassen sich in Tasks auch Schleifen, Variablen und Bedingungen verwenden.



Bild 2.45: *Tasker* bietet bereits von Haus aus eine Vielzahl von Aktionen – und lässt sich mit Plugins (auch denen von *Locale*) erweitern

Im linken Bild sieht man bereits einen Eintrag „Plugins“: Ja, auch Tasker ist in der Lage, mit den zahlreichen *Locale*-Plugins zu arbeiten. Darüber hinaus bieten auch immer mehr Apps direkte Schnittstellen für Tasker: So lässt sich etwa bei *FTPSyncX* (im Kapitel 1.1 *Dateien und Verzeichnisse auf eigener Hardware* vorgestellt) eine Synchronisation anstoßen oder eine Einstellung ändern. Auch für *Dropbox* gibt es diverse Plugins. Und nicht zuletzt lassen sich bei Bedarf sehr maßgeschneiderte Lösungen wie etwa ein Diebstahlschutz (vgl. Anhang A.5) oder Ähnliches realisieren.

Wenn Tasker also das Non-plus-Ultra ist, warum nutzt es dann nicht jeder? Dafür gibt es sicher mehrere Gründe. Die einen schreckt der Preis ab: Mit etwa fünf Euro ist die App nicht ganz billig – wenn auch, am Funktionsumfang und den gebotenen Möglichkeiten gemessen, absolut nicht teuer. Wer jedoch nur einen kleinen Teil dieser Fähigkeiten benötigt, die zudem noch von einem anderen (vielleicht gar kostenlosen) Tool abgedeckt werden, dem kann man es ja wohl kaum verdenken, wenn er sich dann auch für letzteres entscheidet.

Ein weiterer Punkt ist die mit der App verbundene Komplexität: Wenn jemand behauptet, er hätte sich „mal eben *Tasker* installiert und vollständig eingerichtet“, so hat dieser Mensch glatt gelogen. Selbst jemand, der *Tasker* bereits „kennt wie seine Westentasche“, macht dies nicht „mal eben so nebenbei“. Zugegeben: Je besser man sich damit auskennt, desto mehr setzt man damit auch um. Und hätten unsere Androiden einen Temperatur-, Wasser- und einen Kaffeesensor, könnte Tasker mit gerooteten Geräten auch Kaffee kochen (Kontext: Wasser < 90 °C mit Kaffèepulver; Task: Übertakte CPU, starte alle Benchmarks. Exit-Task: Benchmarks stoppen, CPU wieder normalisieren) ...



<http://www.androidpit.de/de/android/forum/thread/435917/>

Zugegeben: *Tasker* mag ein wenig gewöhnungsbedürftig sein und fordert zumindest ein wenig Einarbeitung. Aber auch wenn gelegentlich behauptet wird, man bräuchte dafür ein Diplom: So kompliziert ist es nun wirklich nicht. Und mir ist niemand bekannt, der den kleinen Aufwand zu Beginn später bereut hätte. Um neuen Anwendern den Einstieg zu erleichtern, habe ich im AndroidPIT-Forum eine kleine Sammlung der wichtigsten Ressourcen erstellt – hier finden sich Links zu Tutorials, Wikis und weiteren Hilfsquellen.



<https://tasker.dinglish.net>

Übrigens: *Tasker* gibt es auf der Homepage in einer Gratis-Version für sieben Tage zum Testen. Die Vollversion sollte man anschließend auch dort erwerben: Gegenüber der Playstore-Version kommen dann noch einige Features wie Verschlüsselung hinzu, und außerdem sind die Kosten hier geringfügig niedriger.

2.6 Datei-Manager

Gibt es ihn, den ultimativen Datei-Manager? Viele Anwender werden auf diese Frage ein klares „Ja“ zurückgeben. Nur der Rest der Antwort – nämlich das nebensächliche Detail, um welche App es sich dabei wohl handeln möge – dürfte sehr unterschiedlich ausfallen. Denn was für den einen „ultimativ“ ist, mag für jemand anderen völlig uninteressant sein – das Umgekehrte gilt natürlich ebenso. Doch zum Glück ist auch in diesem Bereich die Auswahl an für Android verfügbaren Apps umfangreich: Angefangen bei solchen, die sich ausschließlich um die SD-Karte kümmern, bis hin zu denen, die nebenbei auch noch den ganzen Rest des Androiden (einschließlich der Hardware) verwalten wollen, ist alles dabei.



<http://www.androidpit.de/de/android/forum/thread/411023/>

Bei einem derart großen Umfang kann ich natürlich nicht jede App vorstellen. Daher werde ich im Folgenden für die mir wichtig erscheinenden Bereiche die aus meiner Sicht besten Kandidaten herausgreifen – eine Auswahl, die natürlich sehr subjektiv ist. Dennoch hoffe ich, damit einen recht guten Überblick zu geben – und niemandem auf die Füße zu treten. Und gleich vorab: Eine Übersicht zu diesem Thema findet sich bei AndroidPIT.

Für den „normalen Anwender“

Mein persönlicher Favorit ist der *ES Datei Explorer* (Bild 2.46). Er bringt alles mit, was man im Alltag wirklich benötigt: In Listen- oder Icon-Ansicht lässt sich das komplette lokale Dateisystem durchforsten. Bilder, Videos und auch verschiedene Dokumente kann

die App gleich anzeigen, ZIP-Dateien ein- und auspacken RAR-Dateien auspacken und mehr. Zugriff auf den heimischen PC aus dem heimischen WLAN heraus? Über **SMB** gar kein Problem, sogar den Server findet **ES** selbst. Mal eben etwas vom FTP-Server holen? Ebenfalls kein Thema. Sogar SFTP (SSH), Bluetooth und Dropbox werden unterstützt.



ES Datei Explorer

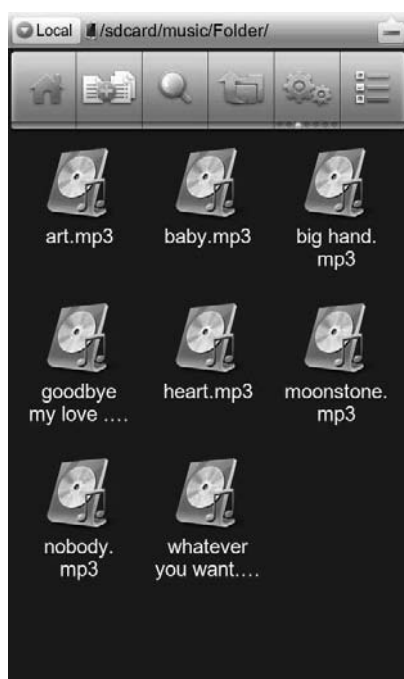


Bild 2.46: *ES Datei Explorer* ist einer der vielfältigsten und beliebtesten Datei-Manager

Aber auch an all die, die gern mehr wollen, ist gedacht: Seit einer Weile beinhaltet die App auch Unterstützung für „Wurzelmenschen“. Ein minimaler Lesezeichen-Manager hilft, wichtige Orte schnell wiederzufinden, und installierte Apps lassen sich auflisten, sichern oder deinstallieren (für Details wird auf das App-Management des Android-Systems zurückgegriffen). Und wem das noch immer nicht reicht, der kann die App mittels weiterer AddOns erweitern: Um einen „großen“ Lesezeichen-Manager, einen Task-Manager, einen Sicherheits-Manager ...

Eine der wenigen Sachen, die ich beim *ES Datei Explorer* erst lange suchen musste, ist die Anzeige von Details zu den Dateien in der Listenansicht. Dies scheint für den **ASTRO Datei-Manager** (Bild 2.47) selbstverständlich zu sein. Davon abgesehen scheint sich der Funktionsumfang dieser beiden Apps annähernd zu decken: Auch **ASTRO** versteht sich auf die Navigation durch das komplette Datei-



ASTRO Datei-Manager

system, einschließlich dem Kopieren, Verschieben oder Löschen von Dateien. Mittels Modulen lässt er sich erweitern, so dass Gleiches auch für Bluetooth, SMB und SFTP gilt. Ein Task-Manager scheint bereits an Bord, und für das Betrachten von Bildern sowie die Verwaltung installierter Apps ist ebenfalls gesorgt.

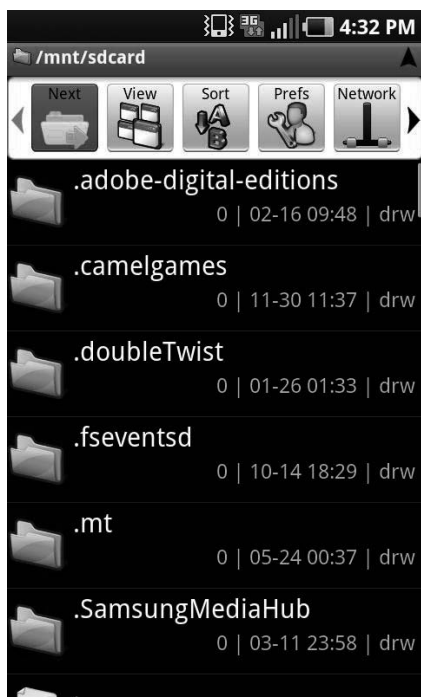


Bild 2.47: Auch der **ASTRO Datei-Manager** erfreut sich großer Beliebtheit und bietet gute Funktionalität

„Wurzeltools“ bringt ASTRO keine mit, und das Design ist sicher Geschmacksfrage. Auf der Beliebtheits-Skala liegen die beiden genannten Apps relativ dicht beisammen, was die Bewertungen im Playstore betrifft.



Total Commander

Doch die Szene könnte durchaus in absehbarer Zeit ein wenig aufgemischt werden, denn einer der bekanntesten Datei-Manager aus der Windows-Welt hat den *Playstore* betreten. Die Rede ist vom **Total Commander** – und der kann sich offensichtlich in Sachen Funktionsumfang mit den beiden anderen vorgestellten Kandidaten durchaus messen. Wie der Screenshot in Bild 2.48 erkennen lässt, kann man durch das lokale Dateisystem ebenso navigieren wie durch SMB-Freigaben. Ein Lesezeichen- sowie ein App-Manager sind zu erkennen, ebenso die Möglichkeit zum Download weiterer Plugins. Die Archiv-Unterstützung (ZIP, RAR) entspricht der des *ES Datei Explorers*; an Netzwerk-Protokollen stehen neben SMB offensichtlich noch FTP und FTPS zur Verfügung (SFTP ist unter Windows eben nicht so verbreitet). Ebenso soll

ein Text-Editor direkt integriert sein. 4,9 Sterne bei über 6.000 Bewertungen (vor allem in sehr kurzer Zeit) legen nahe, dass der *Total Commander* sicher keine schlechte Wahl ist.



Bild 2.48: Ein guter Bekannter aus der Windows-Welt: **Total Commander**

Spezielles für „Wurzelmenschen“ (root)

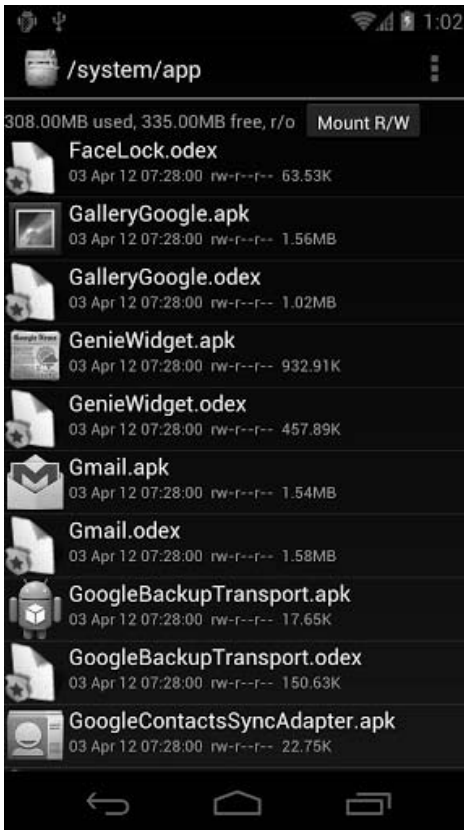
Wie bereits gezeigt, lässt sich der *ES Datei Explorer* auch als „root-Explorer“ nutzen – allerdings noch nicht sehr lange. Auch der **Ghost Commander** ist dazu in der Lage. Dennoch gibt es natürlich Apps, die sich genau auf dieses Gebiet spezialisiert haben.

Eine dieser Apps trägt den Namen **Root Explorer** und ist auf dem Bild 2.49 zu sehen. Selbstredend lässt sich damit das gesamte Dateisystem erkunden – und was nicht schon beschreibbar ist, wird beschreibbar gemacht (wie man dem Button in der rechten oberen Ecke unterstellen darf).



Ghost Commander





Root Explorer

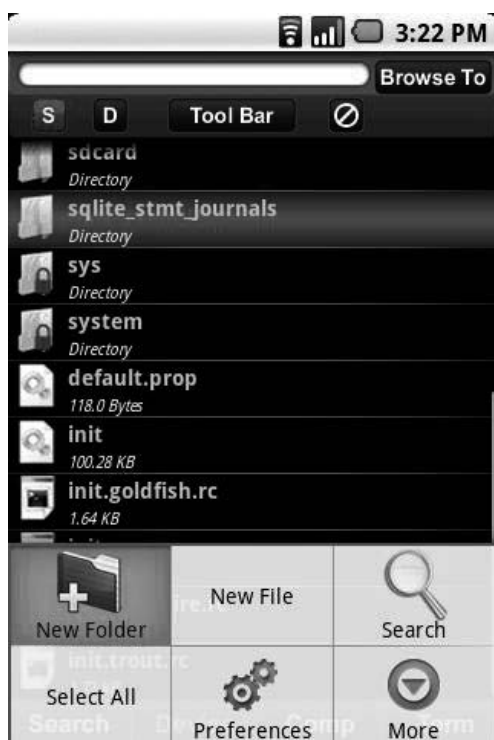
Bild 2.49: *Root Explorer* ist ein Datei-Manager mit speziellen Funktionen für Wurzelmenschen

Doch damit ist das Thema noch lange nicht erschöpft: Mit dabei ist auch ein SQLite Database Viewer, damit man Einblick in die Datenbanken des Systems nehmen kann. Denn davon ist vieles in derartigen Datenbank-Dateien gespeichert – beispielsweise die Anruflisten, die Kurznachrichten, und natürlich auch die Kontaktliste sowie der Kalender. Da sind Dinge wie der integrierte Text Editor, die Möglichkeit zum Erstellen und Entpacken von ZIP sowie Tar/GZip-Dateien bzw. das Auspacken von RAR-Archiven schon fast normal.

Als spezielle **root**-Features kann man das Ausführen von Skripten, (Neu-) Einbinden von Dateisystemen, Ändern von Dateiberechtigungen und -eigentümern sowie den binären APK XML-Viewer betrachten. Lesezeichen und die Möglichkeit, Dateien via Mail, Bluetooth etc. zu versenden, runden das Ganze schließlich ab.

Auch **SU File Manager & Terminal** (Bild 2.50) richtet sich speziell an root-Fans und erlaubt das Einbinden von Dateisystemen, Anpassen von Dateiberechtigungen und das Ausführen von Skripten. Ein Terminal (Kommando-Zeilen-Tool) ist ebenfalls integriert. Der Datei-Manager gibt Zugriff auf alle lokalen Dateisysteme, aber auch über das Netzwerk auf andere Rechner, wobei wahlweise FTP oder **SMB** Verwendung findet.

Ebenso ist es möglich, Textdateien direkt zu editieren, und es lassen sich sogar symbolische Links anlegen. ZIP-Archive werden direkt unterstützt.



SU File Manager & Terminal



Bild 2.50: Auch der **SU File Manager** richtet sich speziell an Power-User mit gerootetem Gerät

Toolboxen mit integriertem Datei-Manager

Um die Sache am anderen Ende zu beginnen: Der bereits zuvor genannte *ES Datei Explorer* lässt sich mit AddOns zu einer derartigen Toolbox ausbauen. Da gibt es einen Lesezeichen-Manager, mit dem sich Bookmarks für Dateien, Verzeichnisse etc. verwalten lassen, einen Task-Manager (einschließlich eines praktischen Widgets) und sogar einen Sicherheits-Manager. Letzterer vermag es, Apps mit Passwort zu schützen, hat einen „Thread Detector“, kann das Gerät aus der Ferne sperren und auch den Standort des Gerätes ermitteln.

Von vornherein in Volllausstattung kommt *eFile* (Bild 2.51) daher – und das gratis und ohne Werbung. Einen Großteil des Funktionsumfangs kann man bereits dem Screenshot entnehmen: Datei-Manager, Task-Manager, App-Manager sowie eine Anbindung zu *eRay* (einem weiteren Tool des gleichen Entwicklers) lassen sich da erkennen.

Der Datei-Manager bietet per FTP und SMB Zugriff auf andere Rechner, kann ZIP-Dateien packen und entpacken sowie RAR-Dateien extrahieren. Suche und Lesezeichen sind



eFile

mit dabei, **APK-Dateien** lassen sich direkt installieren sowie alle möglichen Dateien per Mail-Attachment oder Bluetooth verschicken. Ein Texteditor findet sich hier ebenso wie die Möglichkeit, das Wallpaper oder den Klingelton zu setzen; sogar Shortcuts lassen sich erstellen.



Bild 2.51: eFile bietet neben einem Datei-Manager auch einen App-Manager, Task-Manager und mehr

Advanced Users
Toolbox

Prinzipiell interessant klingt auch **Advanced Users Toolbox** (Bild 2.52): ZIP-Support, App-Installer/Uninstaller, Akku-Manager, Market-History-Cleaner, generischer Cache-Cleaner und mehr gesellen sich hier zum integrierten Datei-Manager. Wer sein Gerät gerootet hat, kommt in den Genuss weiterer Features – wie etwa einem Cleaner für den Dalvik-Cache.

Noch mehr zu bieten scheint **Advanced Tools** (Bild 2.53): An Bord sind u. a. ein Datei-Manager mit ZIP-Support sowie Unterstützung für Bluetooth und FTP, ein System-Manager mit umfangreichen System-Infos und der Möglichkeit, etwa CarrierIQ zu entdecken (falls dieser Spion auf dem Gerät vorhanden ist), App-Manager, Terminal, Sensor-Analyzer, GPS Status & Fix und mehr. Auch hier gibt es auf gerooteten Geräten erweiterte Funktionalitäten – etwa zur Anpassung der Pixeldichte des Displays, Einfrieren von Bloatware und mehr.

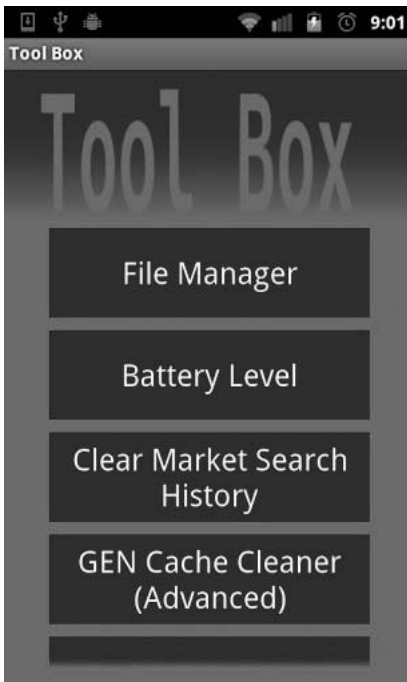


Bild 2.52: Advanced Users Toolbox ist ein gut gefüllter Werkzeugkasten zur Systemverwaltung



Advanced Tools

Bild 2.53: Advanced Tools wartet mit umfangreichen Möglichkeiten auf

Weitere Kandidaten dieser Kategorie finden sich noch in der eingangs genannten Übersicht. Alternativ ist es sicher nicht verkehrt, sich für jeden benötigten Bereich eine App auszuwählen, die sich auf diesen spezialisiert hat und ihre Aufgaben daher mit Bravour löst. Einige davon werde ich im Kapitel 4 dieses Buches zum Thema *Tuning* noch nennen.

2.7 Androiden vom PC aus verwalten

Eine Übersicht zu diesem Thema findet sich *bei AndroidPIT*.



<http://www.androidpit.de/de/android/forum/thread/427833/>

Für den „normalen Anwender“

MyPhoneExplorer (Bild 2.54) ist in diesem Bereich sicher die bekannteste und beliebteste App. Ihre größte Einschränkung ist jedoch, dass sie nur mit einem Windows-Betriebssystem kommunizieren kann, auf dem überdies dafür auch eine spezielle Anwendung installiert sein muss. Mac und Linux-Nutzer stehen also außen vor. In dieser Richtung ist auch nichts geplant; es wird jedoch darauf verwiesen, dass die Software mit einigen Einschränkungen auch unter Wine eingesetzt werden kann.



MyPhoneExplorer

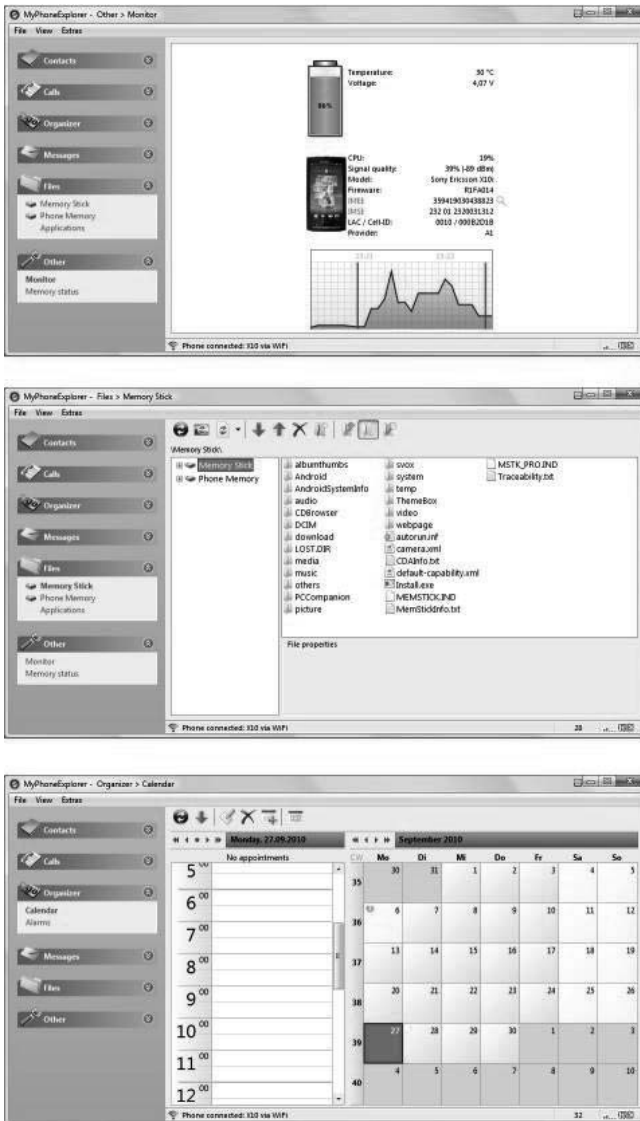


Bild 2.54: MyPhone-Explorer ist die PC-Suite für Windows-Rechner

Die meisten Leser wird diese Einschränkung nicht weiter stören, da sie auf ihren PCs das entsprechende Microsoft-Betriebssystem im Einsatz haben. Und für sie ist der *MyPhone-Explorer* sicher eine gute Wahl. Sehr bequem in der Handhabung, deckt er vieles ab: Verwaltung der Kontakte, Telefonlisten, Kalender und auch SMS, wobei sich auch Anrufe initiieren und SMS lesen/schreiben lassen. Dateien und Medien (Fotos, Videos) lassen sich natürlich ebenso verwalten.

Des Weiteren bietet die App die Möglichkeit, vom PC aus Kurznachrichten zu lesen, zu schreiben, die Kontakte zu verwalten, Screenshots zu erstellen, die WebCam zu nutzen, Apps zu sichern und vieles mehr. Sogar ein persönlicher Web-Server lässt sich damit auf dem Androiden realisieren oder der Zugriff für einen irgendwo in der Ferne sitzenden Spezialisten via Netzwerk-Brücke umsetzen, während man gerade im mobilen Netz unterwegs ist. Beinahe vergessen hätte ich die Möglichkeit, dass sich mit Hilfe von *Remote Web Desktop* PC und Androide eine gemeinsame Zwischenablage teilen können.

Auch der **PAW Server** (Bild 2.56) funktioniert unabhängig von einem speziellen PC und wird einfach im Browser benutzt. Der große Vorteil dieser Tatsache: Man kann ihn überall verwenden – beispielsweise, wenn man bei Freunden/Verwandten zu Besuch ist. Einzig ein funktionierendes WLAN und ein ebenfalls darin eingebuchter Rechner mit Web-Browser werden benötigt. Und da es wohl kaum einen aktuellen PC ohne Webbrowser drauf gibt, wäre eigentlich ausschließlich WLAN als Voraussetzung zu nennen. Im heimischen Netzwerk eingebucht und auf dem Router eine entsprechende Port-Freigabe eingerichtet, kann auf diese Weise gar ein Experte aus der Ferne hilfreich unter die Arme greifen – vorausgesetzt ihm wurden die IP-Adresse und die Zugangsdaten zum **PAW Server** mitgeteilt.



PAW Server

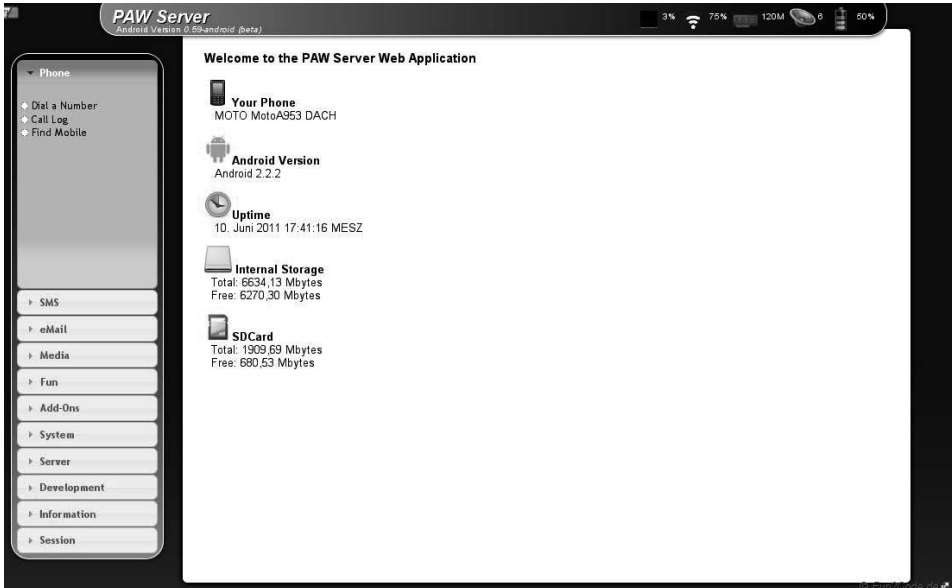


Bild 2.56: Auch den **PAW Server** bedient man im Web-Browser. Diese App bietet zusätzliche Schnittstellen für Programmierer

Wie auch bei den zuvor genannten Kandidaten lassen sich hier Anruflisten, SMS, Kontakte etc. einsehen, Anrufe initialisieren, SMS schreiben etc. Und wenn der Hund sich „den Knochen“ geschnappt und verschleppt hat, lässt sich selbiger per Knopfdruck zum Klingeln bringen (der „Knochen“, nicht der Hund!), um festzustellen, wo er denn nun abgeblieben ist.

Natürlich ist auch ein Datei-Manager enthalten. Fotos lassen sich ebenfalls durchstöbern (auf Wunsch sogar eines davon als neues Hintergrundbild festlegen), der Androide als Diktier- oder Vorlesegerät oder auch Musik-Player oder WebCam nutzen und vieles mehr.

Für den „Power-User“

Die letzten Absätze müsste ich an dieser Stelle nun wiederholen – denn der *PAW Server* ist definitiv etwas für „Power-User“. Besonders interessant für Tüftler: Der integrierte Web-Server kann mit eigenen Skripten ergänzt werden. Dazu bietet sich die *PAW*-eigene Skriptsprache an, aber auch ein PHP-Plugin ist verfügbar. Des Weiteren unterstützt *PAW* auch die genannten Tools *Locale* und *Tasker*.

Kommen wir zu einem kleinen Schmankehl, das besonders Android-Entwicklern gefallen dürfte. Sie sind zwar überwiegend den Umgang mit der **ADB** gewöhnt und setzen sicher so manchen Befehl darüber ab – insbesondere, um Dateien mit `adb push` auf das Gerät bzw. mit `adb pull` vom Gerät herunter zu kopieren. Wer vorwiegend an der Shell unterwegs ist, ist damit sicher durchaus zufrieden, doch so manch einer hat sich dafür vielleicht schon eine kleine grafische Oberfläche gewünscht.

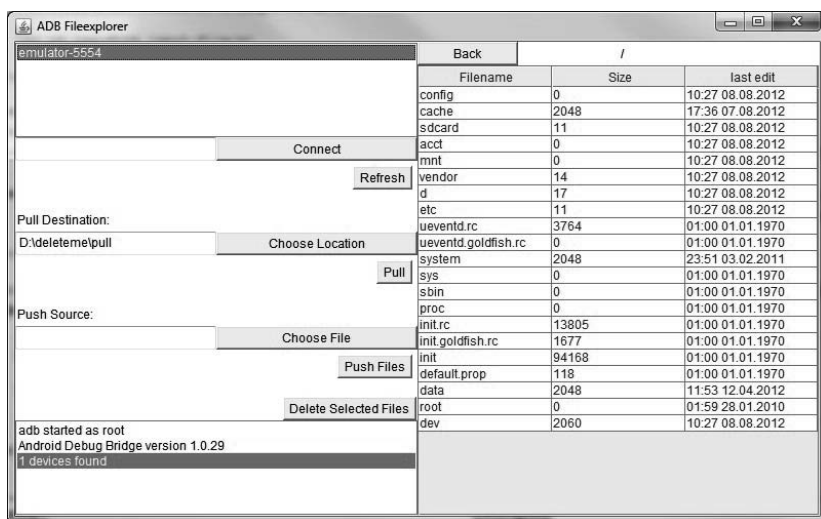


Bild 2.57: Ein per ADB angebundenes Android-Gerät lässt sich bequem mit dem **ADB FileExplorer** erkunden

Diesem Wunsch ist XDA-Forums-Mitglied DareTOBe nachgekommen und hat den *ADB FileExplorer* (Bild 2.57) bereitgestellt. In Java geschrieben, lässt sich dieses Programm unter nahezu jedem Betriebssystem einsetzen. Es ermöglicht das Kopieren von Dateien zwischen Gerät und Arbeitsrechner, das Löschen von Dateien sowie das Browsen durch das Dateisystem auf dem Androiden – und auch das Aufbauen einer ADB-Verbindung über TCP/IP.

Darf es ein wenig mehr sein? Dann wäre vielleicht *ADBBrowser* einen Blick wert. Verfügbar für Windows und Linux (32-Bit sowie 64-Bit), bietet er einen Datei-Browser – aber ebenso auch einen App-Browser. Reicht nicht? Na gut, einen noch: *QtADB* (Bild 2.58). Verfügbar für Windows, Mac und auch Linux (sowohl 32-Bit als auch 64-Bit), ist er mit tollen Features nur so vollgestopft: Datei-Manager, App-Manager, Geräte-Informationen, Verwaltung der SMS, Shell-Zugriff, Screenshots, Logcat, Backup (Nandroid – aber auch einzelne Apps mit und ohne Daten). Und wem es dann wirklich reicht, der findet hier auch eine Möglichkeit zum Reboot.



ADBBrowser



QtADB



Bild 2.58: Mit *QtADB* kann ein per ADB angeschlossenes Android-Gerät nahezu vollständig verwaltet werden

2.8 Custom Recovery und ROMs

Die Begriffe *Recovery*, *ROM* und *Custom-ROM* fielen ja nun bereits des Öfteren. Während die *Begriffserklärungen* im Anhang diese Themen nur grob umreißen, soll an dieser Stelle näher auf die Einzelheiten eingegangen werden.

Custom Recovery: ClockworkMod

Was die Begriffserklärung zu *Recovery* beschreibt, ist eigentlich schon ein *Custom Recovery* – denn was ab Werk daherkommt, ist eher spartanisch. Nur wenige Punkte stehen hier zur Auswahl – insbesondere Dinge wie *Nandroid Backup* oder die Installation von *Custom-ROMs* fehlen hier gänzlich. Ein Werksreset sowie das Einspielen von offiziell angebotenen Updates der Hersteller/Netzanbieter ist jedoch meist möglich.

Wesentlich interessanter wird es dann schon mit einem Custom Recovery, das viele gleich mit dem bekanntesten Kandidaten, dem *ClockworkMod* Recovery, gleichsetzen. Dies ist einfach das verbreitetste Custom-Recovery und für die größte Auswahl an Geräten auch verfügbar. Ein anderes recht bekanntes Custom Recovery wäre das abgebildete *AmonRa* (welches bei der Brutzelstube näher beschrieben – aber lediglich für eine Auswahl an HTC-Geräten verfügbar ist). Da zuerst genanntes *ClockworkMod Recovery* jedoch das verbreitetste ist, möchte ich mich hier darauf beschränken. Ein Vergleich der Screenshots zeigt außerdem bereits, dass der Funktionsumfang sich stark ähnelt.



AmonRa

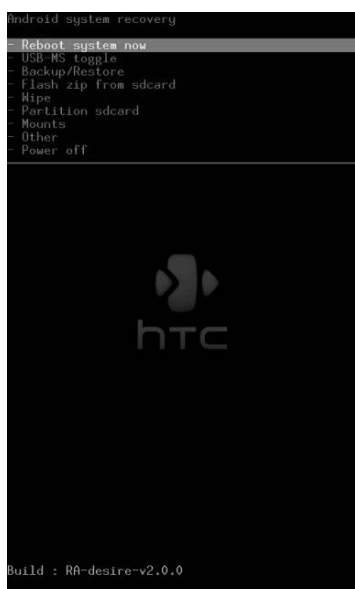


Bild 2.59: *AmonRa* ist ein Custom Recovery für zahlreiche HTC-Geräte

Das von Koushik Dutta (in der Community besser bekannt als *Koush*) entwickelte **ClockworkMod Recovery** (Bild 2.60) bietet gegenüber dem *Stock Recovery* eine ganze Reihe zusätzlicher Funktionalitäten, wie beispielsweise:

- erweiterte Recovery-, Installations- und Wartungsmöglichkeiten
- Backup und Restore (**Nandroid**)
- Installation von Custom-ROMs, Kernels, Mods, u. a. m.
- **Wipe** einzelner/aller Partitionen
- Formatieren einzelner Partitionen
- Löschen der Akku-Statistiken

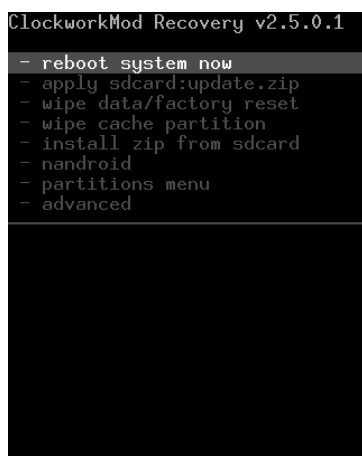


Bild 2.60: Koush's **ClockworkMod Recovery** ist das bekannteste Recovery und für viele Geräte verfügbar

Besonders praktisch bei *ClockworkMod Recovery* ist, dass der Entwickler auch eine Companion-App namens **ROM Manager** bereitstellt, mit der sich viele Aufgaben auch bequem aus dem laufenden System anstoßen lassen. Wie der Screenshot (Bild 2.61) zeigt, lässt sich mit dieser App auch bequem das Recovery-Image installieren. Ebenso findet man hiermit eine Auswahl von Custom-ROMs, die mit dem Gerät kompatibel sind, und kann diese direkt herunterladen und installieren. Ist bereits ein von *ROM Manager* unterstütztes Custom-ROM installiert, findet man mit der App auch heraus, ob etwa Updates verfügbar sind – die sich natürlich dann ebenfalls herunterladen und installieren lassen.

Wer des Englischen mächtig genug ist, dem sei auch ein Video bei Youtube nahegelegt: **Detailed Walk-Through of ROM Manager for Android** gibt eine Video-Tour durch die Möglichkeiten, die *ROM Manager* bietet.



<https://www.youtube.com/watch?v=psml8KmBNeY>



ROM Manager

Wie kann man nun herausfinden, ob *ClockworkMod Recovery* bereits auf dem Gerät installiert ist? Hat man das Gerät gerade neu erworben, erübrigt sich diese Frage sicherlich: Ich habe noch nie gehört, dass ein Hersteller oder Netzbetreiber ein Custom Recovery vorinstalliert hat. Aber sei es drum: Wer ohnehin gern auf den *ROM Manager* zurückgreifen möchte, werfe noch einmal einen Blick auf den Screenshot. Ist nämlich *ClockworkMod Recovery* bereits auf dem Gerät installiert,

wird die installierte Version hier auch gleich im ersten Punkt mit ausgewiesen. Alternativ kann man natürlich auch in den **Recovery-Modus** booten und schauen, ob die erweiterten Funktionalitäten angeboten werden – und die erste Zeile (wie im obigen Screenshot zu sehen) mit „ClockworkMod“ beginnt.



Bild 2.61: *ROM Manager* spielt mit *ClockworkMod* zusammen und erleichtert viele Aufgaben rund um Custom-ROMs

Nandroid-Backups

Auch dieser Begriff ist bereits häufiger gefallen. Was ein Nandroid-Backup ist, haben die meisten Leser, die bis hierher durchgehalten haben, sicher auch bereits bei der Begriffserklärung *Nandroid* im Anhang nachgeschlagen. Doch wie gerade zuvor beim Thema „Custom Recovery“, sollen auch hier nähere Details folgen.

Zuerst einmal nehmen wir das Wort auseinander, denn wer hinter dem Begriff „Nandroid“ ein mit einem „N“ versehenes „Android“ vermutet, liegt leicht daneben. Meine Schuld, zugegeben: Ich hätte es deutlicher schreiben können. Dann sähe das Wort nämlich so aus: NANDroid. Und die ersten vier Buchstaben beziehen sich auf das, was gesichert werden soll: der Inhalt des **NAND-Flash**, den meisten als „interner Speicher“, „Gerätespeicher“, oder auch „Telefon-Speicher“ bekannt. Wie man selbiges aus dem **Recovery Menü** her-

aus erstellt, wurde bereits im Abschnitt zum Thema *Backup* behandelt. Von dort ist auch bereits bekannt, dass dabei die kompletten Dateisysteme gesichert werden – ein solches Backup ist also definitiv ein „Komplett-Backup“. Ebenfalls bereits an betreffender Stelle geklärt wurde die Tatsache, dass sich ein Nandroid-Backup normalerweise nur vollständig wiederherstellen lässt (zumindest aus dem Recovery-Menü heraus); wer einzelne Daten benötigt, kann dazu jedoch auf spezielle Apps zurückgreifen.

Verwendet man zur Erstellung von Nandroid Backups das gerade behandelte *Clockwork-Mod Recovery*, landen die gesicherten Daten im Verzeichnis `clockworkmod/backup/` auf der SD-Karte, wo sie natürlich jede Menge Platz belegen: Schließlich handelt es sich bei jedem Backup um die vollständigen Images der internen Dateisysteme. Daher sollte man hier hin und wieder aufräumen: Während man auch aus Gründen der Datensicherheit eine Kopie dieser Backups auf einem anderen Gerät (z. B. dem heimischen Computer oder NAS) ablegen sollte, muss man auf der SD-Karte schließlich nicht alle Backup-Generationen aufheben. Löschen kann man ältere Backups auf verschiedene Weise:

- mit einem **Datei-Manager** direkt auf dem Androiden
- direkt auf dem Android-Gerät mit zuvor genanntem *ROM Manager* (unter „Manage Backups“)
- vom Computer aus, indem die SD-Karte dort eingebunden wird oder indem man mit einem **Remote-Manager** über WLAN darauf zugreift

In welchem Format die erstellten Backups angelegt werden, hängt vom verwendeten Nandroid-Backup-Tool ab (es handelt sich in der Tat um ein separates Tool, das lediglich in diverse Custom-Recoveries integriert wurde). So ist etwa *ClockworkMod* mit Version 5 dazu übergegangen Tar-Archive zu erstellen. Welches Format man genau vor sich hat, lässt sich i. d. R. jedoch leicht am Dateinamen erkennen:

- `system.ext3.tar`: eine Sicherung der Partition `/system`, deren Dateisystem EXT3 ist, in einem Tar-Archiv
- `data.img`: Image-Datei der Partition `/data`, wobei das Dateisystem nicht angegeben ist (unter **Dateisysteme** wird beschrieben, welche Dateisysteme zum Einsatz kommen)

Und wie kommt man am Computer an die Inhalte eines solchen Backups heran – etwa zur Inspektion einzelner Dateien oder Rettung einzelner Datensätze aus einer der enthaltenen Datenbanken? Bei `.tar`-Dateien ist das klar: Auspacken. Aber wie sieht das etwa bei einem YAFFS2-Image aus? Für Linux-Anwender gibt es da das kleine Tool *unyaffs*, welches das komplette Image entpackt (und zwar in das Verzeichnis, in dem sich auch die Image-Datei befindet).

Auf der Website steht sowohl eine statisch kompilierte Binärdatei zur Verfügung als auch die Möglichkeit, sich den Quellcode zum Selbst-Kompilieren herunterzuladen. Ich

habe mir einmal erstere gegriffen: Sie lief problemlos auf meinem 32-Bit-Ubuntu 8.04 – und läuft noch immer tadellos auf meinem 64-Bit-Ubuntu 12.04 (mit installiertem `ia32-libs`-Paket):

- `unyaffs` als `root` nach `/usr/local/bin` kopieren, damit es im `$PATH` liegt und somit von überall aus verfügbar ist: `sudo cp unyaffs /usr/local/bin`
- die zu entpackende Image-Datei in ein leeres Verzeichnis legen (da `unyaffs` alles immer dort auspackt, wo diese Datei liegt – und nicht in das Verzeichnis, aus dem es aufgerufen wird): `mkdir mydata && cp data.img mydata/`
- in das Verzeichnis wechseln und das Westpaket auspacken: `cd mydata && unyaffs data.img`
- optional: Die Image-Datei wieder löschen (sofern man noch eine Kopie an anderer Stelle liegen hat): `rm -f data.img`
- auf Forschungsreise gehen

Zur Erforschung der zahlreichen Datenbank-Dateien, die überwiegend im SQLite-Format vorliegen, gibt es zahlreiche Front-Ends: An der Kommandozeile arbeitet etwa das Standard-Tool namens `sqlite3`, als grafisches Frontend für Linux, Mac und Windows gibt es auch *SQLiteMan*. Und interessante Datenbanken gibt es zur Genüge:

SMS/MMS:

```
data/com.android.providers.telephony/databases/mmssms.db
```

MultiMedia-Metadaten:

```
data/com.android.providers.media/databases/*.db
```

Kalenderdaten:

```
data/com.android.providers.calendar/databases/calendar.db
```

Und zahlreiche weitere. Viele Apps speichern ihre Daten auf diese Weise, und sie finden sich zumeist unter `data/<Paketname der App>/databases` wieder (der Paketname lässt sich der Google-Play-URL der App entnehmen – er ist dort mit dem Parameter `id=` angegeben). Fröhliches forschen!

Stock ROMs und AOSP

Irgendwo basiert eigentlich jedes Android-System auf dem **AOSP**, dem *Android Open Source Project*, denn dieses stellt schließlich das Kernsystem zur Verfügung. Nun ist es leider nicht einfach damit getan, sich hier den Code herunterzuladen, zu kompilieren und auf dem Gerät zu installieren – zu unterschiedlich ist die Hardware, sodass meist Herstel-

ler- und Geräte-spezifische Anpassungen nötig sind (außer natürlich für die direkt unterstützten Geräte). Und das ist der erste Punkt, in dem sich sogenannte „Stock-ROMs“ von den „originalen AOSP-ROMs“ unterscheiden.

Nebenbei erklärt dies auch viele der Verzögerungen bei Updates: Wenn das AOSP-Team eine neue Android-Version fertiggestellt hat, müssen die Hersteller ja noch ihre spezifischen Hardware-Anpassungen (Treiber etc.) vornehmen. Das ist jedoch nur einer der Gründe, denn schließlich haben sie ja (dank Open Source) bereits während der Entwicklung Zugriff auf den AOSP-Code und könnten so auch etwas zeitiger mit ihren Anpassungen beginnen. Da jedoch die meisten Hersteller mehr als nur ein Gerät im Rennen haben, müssen diese Anpassungen auch für mehrere Geräte durchgeführt werden.

Aber es gilt ja nicht nur, die Hardware-spezifischen Dinge anzupassen: Da wären ja auch noch die Hersteller-spezifischen Benutzeroberflächen. HTC Sense, Motorola MotoBlur, Samsungs TouchWiz und wie sie alle heißen – auch sie müssen mit den „neuen Gegebenheiten“ klarkommen. Bis hierher ist das noch einzusehen; doch dann wäre da noch die sogenannte **Bloatware**, die noch mit rein muss: Apps, die weder vom AOSP noch von der spezifischen Benutzer-Oberfläche zwingend benötigt werden, von denen man aber meint, dass die Anwender (also wir) nicht ohne sie leben können. Facebook, Twitter, Peep, die ach-so-tolle Aktien-App (die insbesondere für Europäer wenig interessant ist, da sie nur NASDAQ kennt) – alles Dinge, die sich der Anwender, so er sie denn wirklich braucht, auch bequem über den Playstore installieren kann. Nicht nur, dass viele dieser Apps nerven und Ressourcen fressen, wirklich loswerden kann man sie wieder nur mit *root*. Und Apps wie *su* oder *SuperUser*. apk sucht man bei der Bloatware vergebens.

Eine weitere Ebene bekommen dann noch diejenigen, die ihr Gerät „mit einem Rabatt“ bei ihrem Netzbetreiber erworben haben: Dieser möchte natürlich auch noch seinen Senf dazugeben. Oder eher seinen Brandy – nämlich das sogenannte *Branding*. Das alles muss natürlich bei einer neuen Android-Version auch wieder alles angepasst werden, womit klar ist, warum man hier besonders lange warten darf: AOSP-ROM → Stock-ROM des Herstellers → Stock-ROM des Netzbetreibers. Genau genommen sollte man hier also eigentlich nicht nur vom „Stock-ROM“ sprechen, sondern drei verschiedene Typen unterscheiden:

- AOSP-ROM (auch als „plain Vanilla“ bezeichnet): das originale ROM des AOSP. Leider ohne spezielle Anpassungen nicht auf allen Geräten lauffähig
- Stock-ROM: das vom Hersteller an die Hardware angepasste (und mit einiger Bloatware angereicherte) AOSP-ROM – natürlich passend zum Gerät
- Vendor-ROM: das vom jeweiligen Netzbetreiber angepasste (und mit weiterer Bloatware angereicherte) Stock-ROM – auch passend zum Gerät, nur viiiiel später ...

Custom-ROMs

Nachdem das Thema der „offiziellen“ ROMs geklärt ist, wenden wir uns den Custom-ROMs zu. Aus dem Namen ließe sich bereits zweierlei schließen: Dass sie angepasst (aus dem Englischen „to customize“ – was nicht direkt „kostümieren“ heißt, auch wenn das oftmals ein Nebeneffekt ist) und/oder auf den Kunden (Englisch: „customer“) zugeschnitten wurden. Beides ist in gewisser Weise richtig.

Zu unterscheiden sind hier im Wesentlichen zwei Gruppen: Die einen basieren auf dem **AOSP-ROM** (und pflegen die gerätespezifischen Treiber-Anpassungen selbst nach), die anderen nehmen eher das Stock-ROM des Herstellers als Grundlage. Bekanntester Vertreter ersterer Gruppe ist sicher *CyanogenMod*, das gleich noch separat behandelt wird. Für letztere Gruppe gibt es dann fast so viele ROMs wie Geräte.

Was zeichnet nun ein Custom-ROM aus? Meist kommt es bereits in gerooteter Form daher. Und oftmals läuft es stabiler und performanter als jegliches für das gleiche Gerät verfügbare Stock-ROM, da es besser optimiert und an die Hardware angepasst wurde. Doch auch die **Bloatware** spielt hier eine Rolle: Die meisten AOSP-basierten ROMs lassen diese nämlich weg, einschließlich der Hersteller-spezifischen grafischen Aufsätze. Dass dann weniger ungenutzte Apps und Dienste ständig im Hintergrund mitlaufen, kommt natürlich der Performance zugute. Stattdessen findet dafür die eine oder andere wirklich nützliche App ihren Weg in das ROM – wie etwa bereits zuvor genannter ROM-Manager.

Bei den Stock-ROM-basierten Kandidaten bleibt hingegen die Bloatware in der Regel drauf, die Hersteller-spezifische Oberfläche ohnehin. Worin dann hier die Vorteile liegen? In Optimierungen und Anpassungen sowie hin und wieder auch aktuelleren Android-Versionen. So kann es durchaus passieren, dass ein Hersteller für ein Gerät keine neueren Android-Versionen mehr bereitstellt, für ein anderes – relativ baugleiches – jedoch schon. Hier genügen dann oftmals geringfügige Anpassungen, um auch das „alte Eisen“ wieder mit „jüngeren Gemüse“ zu bestücken.

Und wie steht es um die Update-Geschwindigkeit? AOSP-basierte Custom-ROMs bieten neuere Android-Versionen fast ausnahmslos weit früher an als die Geräte-Hersteller oder gar Netzanbieter. Oftmals gibt es noch Updates für Geräte, welche die Hersteller schon längst abgeschrieben haben (für die es also gar keine „offiziellen“ Updates mehr gibt).

Klingt gar nicht so verkehrt – aber wo bekommt man so ein Custom-ROM her? Die meisten finden sich sicher bei den **XDA Developers**. Wobei „finden“ dabei das eigentliche Problem darstellt: Das richtige ROM für ein bestimmtes Gerät aufzuspüren, ist gerade bei einem derart großen und aktiven Forum nicht sonderlich einfach. Wie gut, dass es auch dafür spezielle Anlaufstellen gibt:

PDADB: Lange Liste (weit über 800 Seiten) für Geräte aller Art – allerdings einschließlich Blackberry, Symbian und so weiter. Keine Filter-Möglichkeit, daher recht unhandlich.



http://pdadb.net/index.php?m=repository&list=rom_update

CommunityRelease: Diese Liste lässt sich explizit nach Gerät, gewünschter Android-Version sowie Entwickler filtern.



http://db.communityrelease.com/androidspin_release_matrix.asp

TheUnlockr: Gruppiert nach Herstellern und sodann nach Gerät. Scheint sowohl recht aktuell als auch recht vollständig zu sein – m. E. die beste Online-Anlaufstelle!



<http://theunlockr.com/downloads/android-downloads/android-roms/>

Man nutzt einfach bereits genannten *ROM Manager*, der die ihm bekannten mit dem Gerät kompatiblen ROMs anzeigt, auf Wunsch herunterlädt und auch gleich installiert – sicher die bequemste Variante.

100% vollständig ist sicher keine der genannten (oder auch ungenannten) Übersichten – das wäre auch nahezu unmöglich. Doch eine gute Auswahl stellen sie alle dar.

CyanogenMod

CyanogenMod ist mit Sicherheit das bekannteste Custom-ROM – und der ständig erwähnte *ROM Manager* findet natürlich automatisch die aktuellste verfügbare Version auf dem eigenen Gerät (sofern es unterstützt wird). Offiziell unterstützt werden mittlerweile über 80 verschiedene Smartphones und Tablets verschiedener Hersteller. Gehört das eigene Gerät nicht dazu, findet sich oftmals eine passende „inoffizielle Portierung“, die nicht selten irgendwann ihren Weg in die „offizielle Liste“ nimmt. Über zwei Millionen Installationen (und der Zähler tickt in rasender Geschwindigkeit weiter) sprechen für sich.



CyanogenMod-Logo

Wie bereits zuvor erwähnt, basiert *CyanogenMod* direkt auf dem AOSP-Code: Hersteller-spezifische Benutzeroberflächen findet man hier also nicht, ebenso wenig die „tolle“ vorinstallierte **Bloatware**, obwohl man selbige hier dank *root* (der ja gleich frei Haus mitgeliefert wird) recht einfach wieder loswerden würde.

Stattdessen legt das Team um Steve Kondik eher Wert auf sinnvolle Anpassungen und Ergänzungen, die jeder im Alltag benötigt – oder die zumindest keinen, der sie nicht benötigt, durch zusätzlichen Ressourcen-Verbrauch belästigen. Um ein paar der (aus meiner Sicht) wesentlichsten Punkte aufzuzählen:

- Lockscreen-Gesten: Statt erst den Bildschirm zu entsperren, dann auf den Home-screen zu wechseln, den App-Drawer zu öffnen, zu suchen etc., definiert man für seine häufig benutzten Apps einfach Gesten und malt beispielsweise ein „M“, um automatisch den Bildschirm zu entsperren und die Mail-App aufzurufen. Oder die Mal-App – je nach Vorliebe.
- Phone-Goggles: Schützen u. a. davor, unbeabsichtigt anzurufen, indem sie eine Sicherheits-Abfrage („Wollen Sie wirklich...?“) einblenden. Wem das noch nicht reicht, der kann auch eine Rechenaufgabe zwischenschalten lassen. Das Ganze lässt sich sowohl auf Zeitfenster als auch auf Rufnummern eingrenzen.
- OpenVPN: für mehr Sicherheit
- Incognito Mode: für „unerkanntes Surfen“, welches (möglichst) keine Spuren hinterlässt: Keine History, und Kekse werden bei Verlassen gleich wieder gelöscht
- DSP Equalizer: für besseren Sound
- Vorinstallierte Apps: wie beispielsweise *Spare Parts* für tiefgreifendere Konfiguration und weitere – aber nichts, was (ohne ausdrücklichen Anwender-Wunsch) am Akku nuckelt oder das System ausbremst.

Und bevor jemand fragt: Ja, ich weiß, dass CyanogenMod mittlerweile ein neues Maskottchen hat. Mit gefällt aber nun einmal der Andy auf dem Skateboard.

Wem das jetzt noch nicht „customized“ genug ist: Da wäre noch ein Ableger zu nennen, der seinerseits wieder auf *CyanogenMod* aufbaut. **AOKP** (Android Open Kang Project) nimmt noch weitere Anpassungen vor und ermöglicht dem Anwender auch zusätzliche Einstellungen. Allerdings ist hier die Anzahl unterstützter Geräte mit knapp 30 geringer als bei *CyanogenMod*.

3 Netzwerk

Der dritte Teil des Buches beschäftigt sich intensiver mit Netzwerk-spezifischen Dingen.

3.1 Netzwerk-Konfiguration

Ganz allgemein sind einige der hier relevanten Themen bereits im zweiten Teil dieses Buches (Abschnitt 2.4 *Konfiguration*) aufgeführt worden – ohne jedoch auf die relevanten Details näher einzugehen. Letzteres soll nun an dieser Stelle nachgeholt werden. Soweit möglich, sollen dabei Bordmittel zum Einsatz kommen. Wo es sich anbietet (etwa weil es kein Bordmittel gibt oder sich etwas auf andere Weise viel bequemer erledigen lässt), kommen auch spezielle Apps zur Sprache.

An und Aus

Da man nicht alle Netz-Dienste ständig benötigt – manchmal sind sie sogar explizit unerwünscht, etwa weil sie wie das Roaming im Ausland zusätzliche Kosten verursachen oder bei gerade nicht verfügbarer Lademöglichkeit zu sehr am Akku nuckeln –, haben vier Dinge unsere spezielle Aufmerksamkeit: WLAN, mobiles Netz (ganz allgemein und Roaming im Speziellen), Bluetooth und – nicht lachen – das Telefonnetz.



Bild 3.1: Android Systemeinstellungen: ***Drahtlos und Netzwerke***. Hier lässt sich auch das WLAN an- und ausschalten

Wie war das jetzt? Frage an Radio Eriwan: „Warum sollte jemand das Telefonnetz abschalten wollen? Das ist doch bei einem Telefon die zentrale Eigenschaft!“ – „Im Prinzip schon, aber ...“ War da was? Eingehende Telefonate im Ausland? Ein eBook im Flugzeug lesen? Ungestörte Nachtruhe bei Verfügbarkeit des morgendlichen Weckers? Also gut: Es gibt auch für die Deaktivierung der telefonisch-kommunikativen Eigenschaften offensichtlich hin und wieder vernünftige Gründe. Schauen wir also einmal nach, wo sich bei Verwendung von Bordmitteln die nötigen Schalterchen versteckt haben.

Im Menü, das sich (wie beschrieben) vom Home-Screen über *Menü* → *Einstellungen* → *Drahtlos & Netzwerke* erreichen lässt, finden wir gleich mehrere Kandidaten. Als Erstes wäre da der *Flugzeugmodus*. Bei diesem handelt es sich um einen „Sammelschalter“, der gleich mehrere Komponenten lahmlegt: Telefon und WLAN im Wesentlichen. Wobei sich das WLAN im Flugzeugmodus meist wieder separat aktivieren lässt – mit dem Punkt unmittelbar darunter beispielsweise. Der Flugzeugmodus versetzt den Androiden in einen sehr stromsparenden Modus: Bei abgeschaltetem Bildschirm wird fast kein Strom mehr verbraucht. Nur ganz abschalten wäre noch sparsamer. Daher bietet sich dieser Modus für eine ungestörte Nachtruhe an, aus welcher der Wecker den Schlummernden allerdings morgens wieder zurückholen soll.

Ungefähr in der Mitte des Screenshots findet sich dann auch König Blauzahn. Wer kein passendes Headset sein eigen nennt und auch sonst keine Bluetooth-Geräte einsetzt, kann den Haken an dieser Stelle gleich permanent entfernen. Ganz am Ende gibt es schließlich den „Knopf“ für das mobile Datennetz.

Nicht mehr auf dem Screenshot zu sehen ist ein weiterer Punkt, bei dem es um die Details für das Mobilfunknetz geht. Dort lassen sich u. a. auch Einstellungen für das Daten-Roaming vornehmen: Soll es verwendet werden oder besser nicht? Die meisten von uns werden es sicher eher abschalten und nur im Ausnahmefall aktivieren. Bei Geschäftsreisenden mag das naturgemäß etwas anders aussehen. Aktiviertes Datenroaming erkennt man im Ausland übrigens an einem „R“ in der Notification-Bar.

Da wir gerade beim Thema „Roaming“ sind: Für die Telefonie ist der Haken, dass es da keinen „Haken“ gibt. Dennoch existieren natürlich Möglichkeiten, sich auch um dieses zu kümmern: entweder indem man im Ausland den Flugzeugmodus aktiviert und bei Bedarf WLAN anschaltet oder *vor* der Abreise (also noch zu Hause) die automatische Betreiberwahl deaktiviert und stattdessen den eigenen Anbieter fest einstellt. Dies funktioniert ebenfalls im zuletzt genannten Menü, unter dem Punkt „Netzbetreiber“.

Eine andere Art von „Netzwerk“ stellt das **GPS** dar, welches bereits in Abschnitt 2.5 unter *Standort und Sicherheit* beschrieben wurde und daher hier lediglich der Vollständigkeit halber noch einmal erwähnt werden soll.

Wer sich nicht ständig durch die vielen Menüs der „Bordmittel“ hangeln möchte, um „eben einmal schnell“ etwas an- oder auszuschalten: Natürlich gibt es dafür bequeme Wege. So sind die wichtigsten Dinge in **Apps mit Schnellzugriffen** enthalten – und

vor allem gibt es auch **Schnellumschalter**, wenn es nur um ein „Umschalten“ (an/aus) geht.

Datensynchronisation im Hintergrund

Ein Smartphone hat man schließlich nicht zuletzt, um auch unterwegs immer auf dem aktuellen Stand zu sein. Viele Apps synchronisieren dafür Daten im Hintergrund. Das ist zwar einerseits recht nützlich, aber nicht unbedingt immer erwünscht. Für einige Apps lässt sich diese Synchronisation daher im Menü *Konten & Synchronisierung* abschalten (per Default ist sie für jede App angeschaltet). An dieser Stelle verewigen sich vor allem die Google-Apps wie *Google Mail* oder der Kalender, aber auch die Hersteller-Apps wie *HTC Sync* (ebenso deren Nachrichten- und Wetter-App) oder Motorolas *MotoBlur*.

Doch nicht alles, was im Hintergrund Daten austauscht, ist an dieser Stelle auch aufgeführt. Ein klassisches Beispiel sind die meisten RSS-Reader. Wer also Einfluss auf den gesamten „Hintergrund-Verkehr“ nehmen möchte, sollte die Einstellungen der verbleibenden Apps separat durchgehen: Bei vielen lässt sich die Häufigkeit der Aktualisierungen einstellen; bei manchen darüber hinaus auch auf ein verfügbares WLAN einschränken.

Mehr zum Thema „Datensynchronisation im Hintergrund“ findet sich im Kapitel 4 *Tuning* unter *Hintergrunddaten und Synchronisierung*.

WLAN-Konfiguration

Besonders viel lässt sich mit dem unter *Drahtlos und Netzwerke* verfügbaren Menü der Bordmittel nicht einstellen. Allenfalls die „Basics“ sind hier verfügbar: WLAN aktivieren? Bei verfügbaren offenen WLANs benachrichtigen? Dazu bei aktiviertem WLAN noch eine Liste der in Reichweite befindlichen Netze mit der Möglichkeit, sich zu verbinden und allenfalls noch den ggf. notwendigen Netzwerkschlüssel einzugeben. Unter „Netzwerke verwalten“ lassen sich auch gerade nicht mehr benötigte, aber konfigurierte Netzwerke (also die, zu denen man bereits einmal verbunden war) entfernen. Mehr ist auf Anhieb nicht ersichtlich. Haben wir da etwas übersehen?

In der Tat. Da war doch am Androiden noch so eine Menü-Taste? Richtig: Dort findet sich ein Punkt „Erweitert“. Und was sich dahinter verbirgt, zeigt der Screenshot in Bild 3.2. In der „Rechtlichen Domain“ gibt man an, wie viele Kanäle benutzt werden dürfen – dies unterscheidet sich nach den lokalen Gesetzen, in Deutschland sind es 13 Kanäle. Weiterhin lässt sich der für **Peer-to-Peer** zu verwendende Kanal einstellen. Interessant ist ferner die „WLAN Standby-Richtlinie“, mit der man festlegt, wann das aktivierte WLAN temporär deaktiviert werden soll. Zur Auswahl stehen hier „bei Display-Aus“, „nie wenn im Netzbetrieb“ oder „niemals“. Wer vermeiden möchte, dass das Internet-Radio im Hintergrund ausgeht, findet hier den richtigen Schalter.



Bild 3.2: Android-Systemeinstellungen: *Erweiterte WLAN-Einstellungen*

Letztlich können auch IP-bezogene Einstellungen getroffen werden. Voreingestellt ist hier die Verwendung von **DHCP**, was in den meisten Fällen auch genau das richtige ist. In manchen Umgebungen ist jedoch eine feste IP notwendig sowie die damit verbundene manuelle Konfiguration von Dingen wie „Default-Gateway“ und „DNS Server“ (wer mit diesen Begriffen nichts anfangen kann, braucht das i. d. R. auch nicht). Der Haken an der Sache: Diese Einstellungen gelten global, also unabhängig davon, mit welchem Netz man gerade verbunden ist. Damit sind sie in der Praxis relativ unbrauchbar.

Abhilfe schaffen kann da beispielsweise **Wifi Static** (Bild 3.3). Mit dieser App lassen sich statische Einstellungen an einzelne Netzwerke binden. Wie der Screenshot erkennen lässt, wechselt die App dann diese Einstellungen auch automatisch, sobald man selbst das Netzwerk wechselt – so sollte das eigentlich von Haus aus sein!

Besonders im „Corporate“-Bereich interessant sind darüber hinaus Apps wie der **WiFi Advanced Config Editor**, mit dem sich WPA-Enterprise-Parameter wie `wpa_supplicant` oder auch der Index des WEP-Schlüssels festlegen lassen.

Wer weitere Apps aus diesem Bereich sucht, mag sich vielleicht für den passenden Post im Forum bei AndroidPIT interessieren.



WiFi Advanced
Config Editor



<http://www.androidpit.de/de/android/forum/thread/429837/>

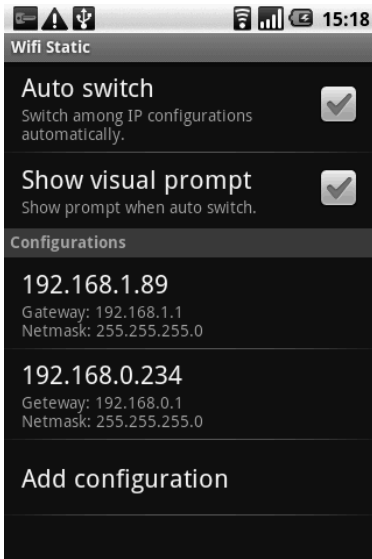


Bild 3.3: *Wifi Static* schaltet zusätzliche WLAN-Einstellungen frei

3.2 Administration

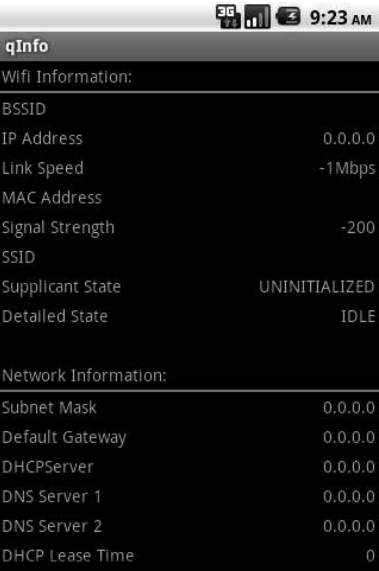
Genau genommen, gehört die Konfiguration natürlich auch zu den Aufgaben eines Administrators – doch meist wird erst nach ihm geschrien, wenn es irgendwo klemmt. Genau da soll dieses Kapitel ansetzen: Was tun, wenn etwas nicht tut? Welche Hilfsmittel gibt es, um die Ursache(n) eines Netzwerk-Problems zu finden?

Geräte-Informationen abfragen

Zuallererst wären da die Geräte-Informationen, von denen sich einige mit Bordmitteln auslesen lassen – an gefühlten zehn verschiedenen Stellen verteilt: Zunächst unter *Einstellungen* → *Telefoninfo* → *Status MAC-Adressen*, Mobilnetz-Typ und Signalstärke. Dann unter *Einstellungen* → *Drahtlos & Netzwerke* das verbundene WLAN-Netzwerk und ggf. auch IP-Adressen. Weitere Details lassen sich dem Gerät eventuell noch mit diversen *Geheimen Zugriffs-Codes* (vgl. Anhang) entlocken. Und bevor die letzten Notizen auf dem Zettel angekommen sind, hat der Nachwuchs selbigen bereits zum Malen mit den Buntstiften entführt.

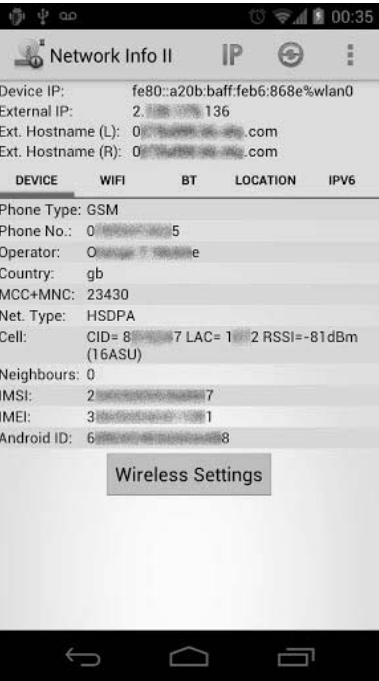
Zum Glück gibt es auch in diesem Bereich wieder eine ganze Reihe Helferlein, von denen ich einige kurz vorstellen möchte. Das Meiste des soeben aufgeführten fasst beispielsweise *qNetInfo* (Bild 3.4) zusammen, jedenfalls soweit es das WLAN betrifft: MAC-Adresse, Signalstärke, verbundenes Netz, zugehörige IP-Adressen und sogar den „Supplicant Status“

(für die Meisten weniger wichtig, aber im „Corporate Context“ durchaus relevant). Damit hat sich der Funktionsumfang dieser nicht einmal 20kB umfassenden App aber auch bereits erschöpft.



qNetInfo

Bild 3.4: qNetInfo zeigt Netzwerk-Einstellungen an



Network Info II

Bild 3.5: Network Info II gibt tieferen Einblick in Netzwerk-Informationen

Ein paar zusätzliche Informationen bietet **Network Info II** (Bild 3.5). Nicht nur WLAN und die mobile Verbindung sind voll abgedeckt, der Entwickler hat auch daran gedacht, dass Bluetooth ebenfalls ein Netzwerk-Interface ist, dass es IPv6 gibt und das mobile Netz darüber hinaus auch Informationen über Mobilfunkzellen bereitstellen kann. Das alles ist sauber auf verschiedene Reiter aufgeteilt, was einen gezielten Zugriff auf die Informationen möglich macht. Wer die gesammelten Informationen gern in Textform exportieren möchte, erhält dazu natürlich die Möglichkeit. An alles ist gedacht, und ich habe mit dieser Beschreibung wohl nur an der Oberfläche gekratzt.

Derart gewappnet, kann man sodann weiterschreiten zum nächsten Schritt – sofern die gewonnenen Erkenntnisse das Problem nicht bereits gelöst haben.

Diagnose: Was geht schief?

In welcher Richtung an dieser Stelle geforscht werden muss, hängt natürlich ganz vom Problem ab: Ist es einfach nur langsam oder kann gar keine Gegenseite erreicht werden (obwohl eine Netzwerk-Verbindung besteht)? Oder kann gar keine Netzwerkverbindung aufgebaut werden? Aber eines nach dem anderen ...

Keine Netzwerk-Verbindung möglich

In diesem Fall greifen wir zunächst auf die *Geräte-Informationen* zurück und schauen erst einmal nach, ob überhaupt eine Gegenseite gefunden wurde. Für WLAN eignen sich die Bordmittel dafür recht gut: Unter *Einstellungen* → *Drahtlos & Netzwerke* → *WLAN-Einstellungen* sollten im Abschnitt *WLAN-Netzwerke* die verfügbaren (d. h. in Reichweite befindlichen) WLAN-Netze aufgelistet sein, zusammen mit Signalstärke und ggf. Verschlüsselungstyp.

Bleibt diese Liste leer, kann es dafür mehrere Gründe geben:

- Es sind schlicht und ergreifend keine WLAN-Netze in Reichweite.
- WLAN ist nicht aktiviert (das Häkchen weiter oben auf der Seite oder der Netzschalter des heimischen Routers).
- Das Netzwerk-Interface ist defekt (entweder im Androiden oder im Router).

Der erste Punkt lässt sich am besten mit einem „Zweitgerät“ verifizieren: Zeigt dieses verfügbare Netze an, muss die Ursache eine andere sein. Auch das Häkchen auf der Einstellungsseite des Androiden ist schnell geprüft, ebenso der Netzschalter des Routers. Dann bleibt nach dem Ausschlussverfahren noch der Fall, dass verfügbare Netze angezeigt werden, aber der Androide sich nicht zu diesen verbinden möchte. Auch das kann sich auf verschiedene Weise äußern:

- Es sieht zunächst danach aus, als würde die Verbindung aufgebaut – doch plötzlich stehen alle Netze auf „außer Reichweite“.
- Eine Fehlermeldung zeigt den fehlgeschlagenen Verbindungsaufbau an.

Der erste Fall ist aus dem Leben gegriffen (tritt beispielsweise oft nach Installation des Custom-ROMs von *CyanogenMod* auf dem *HTC Wildfire* auf). Dann liegt das Problem häufig im Radio-Image begründet; wenn man also seinen Androiden gerootet und mit einer Custom-Firmware versehen hat, hilft meist ein erneutes Flashen des originalen Radio-Images. Doch zuvor erkundigt man sich besser im Forum, da weitere Details entscheidend für den Erfolg sein können.

Der zweite Fall kann mehrere Ursachen haben. Besonders häufig sind:

- falscher Netzwerk-Schlüssel (also so etwas wie ein „falsches Passwort“)
- richtiger Netzwerk-Schlüssel, aber beim falschen Netzwerk eingetragen (läuft auf das Gleiche hinaus)
- ein „MAC-Filter“ beim Zielnetzwerk („Betriebsfremden ist der Zutritt verboten!“)

Am einfachsten lässt sich der zweite Punkt ausschließen, indem man bei der Auswahl des Zielnetzes im zweiten Anlauf besonders genau aufpasst. Sowohl für den ersten als auch für den dritten Punkt muss man sich an den Admin des Routers wenden: Er sollte sowohl den korrekten Schlüssel benennen/mitteilen als auch ggf. die MAC-Adresse des Androiden in die Liste zugelassener Geräte aufnehmen können.

Minimal anders sieht es aus, wenn es sich um das mobile Datennetz handelt: Hier finden sich die Einstellungen unter *Einstellungen* → *Drahtlos & Netzwerke* → *Mobilnetze*, und man kann keinen falschen Schlüssel beim richtigen Netzwerk (oder umgekehrt) eingeben, da die Verifikation über die SIM-Karte erfolgt. Lässt sich kein Kontakt herstellen, hilft neben einer Überprüfung des Häkchens für die Aktivierung des mobilen Datennetzes noch die Verifikation der APN-Daten. Schafft auch das keine Lösung, bleibt der Anruf beim Anbieter der SIM-Karte übrig.

Server können nicht erreicht werden

Ist ein Server nicht zu erreichen, kann dies mehrere Ursachen haben. Möglich wären unter anderem folgende Probleme:

- Der Androide selbst hat keine Netzwerk-Verbindung (siehe oben).
- Der betreffende Server wurde (z. B. für Wartungsarbeiten vorübergehend) heruntergefahren oder gar permanent abgeschaltet.

- Der Server an und für sich ist schon erreichbar, nur nicht der gewünschte Service (Beispiel: Beim Zugriff auf eine Webseite kommt der Fehler, der Server sei nicht verfügbar – Grund ist jedoch nicht ein abgeschalteter Rechner, sondern lediglich die Web-Server-Applikation wurde beendet).
- Der Server läuft wahrscheinlich noch, aber das Netz, in dem er steht, ist nicht erreichbar (defekter Router auf der Strecke).

Während sich der erste Punkt noch lokal klären lässt, sieht der Rest zunächst komplizierter aus: Nicht immer kennt man den Betreiber persönlich, um mal kurz anzurufen und nachzufragen. Wie kommt man der Sache aber sonst auf die Spur? Einige passende Tools sind wiederum in einer Übersicht bei AndroidPIT zusammengefasst, eine kleine Auswahl davon kommt hier zur Sprache.

So lässt sich der Weg zum Zielrechner beispielsweise mit **Traceroute** (Bild 3.6) nachverfolgen. Endet die angezeigte Liste mit der IP-Adresse des gewünschten Ziels, so ist der Server selbst am Netz und vermutlich der Service (also Web-App, Mail oder was immer man benutzen wollte) das Problem. Nicht selten jedoch bleibt der Zug auf der Strecke stehen: Plötzlich dauert es länger, bis die nächste Zeile erscheint und/oder es kommen nur noch Sternchen. In dem Fall ist das Routing (und wahrscheinlich in irgendeinem Rechenzentrum ein Router) defekt; da gibt es nicht viel, was man tun kann. Außer die „defekte Stelle“ liegt noch im Bereich des eigenen Netzanbieters: Dann kann man diesen mit den ermittelten Details kontaktieren und um Hilfe bitten.



<http://www.androidpit.de/de/android/forum/thread/436644/>



Traceroute

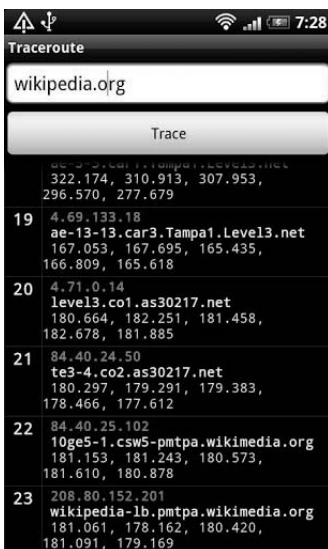


Bild 3.6: Mit **Traceroute** lässt sich die Route zum Zielrechner ermitteln

Zugegeben: Mit derartigen Zahlen- und Zeichenketten ist der Laie nicht selten überfordert. Es fällt einfach schwer, sich darunter etwas vorzustellen. Sicher lässt sich die Ausgabe-Syntax erklären: Die erste Zahl ist einfach ein Zähler (der wievielte Schritt auf dem Weg ist es?), gefolgt von einem Doppelpunkt. Hinter diesem folgen IP-Adresse und, sofern verfügbar, der zugehörige Rechnername. Der „große Bruder“ auf dem PC hätte zusätzlich noch angezeigt, wie schnell die Reaktionszeit war.



Visual Traceroute

Weitaus anschaulicher stellt **Visual Traceroute** (Bild 3.7) diese Informationen dar: Darunter kann sich auch ein Laie etwas vorstellen! Die Route wird bei dieser App auf einer Karte angezeigt, allerdings eher grob, indem die Standorte der Stationen mit direkten Linien, die nicht unbedingt der Kabelführung entsprechen, verbunden werden. Dazu gibt es die gleichen, zuvor genannten Details: Im Bild in den „blauen Bällen“ zur Rechten die Schrittnummer, links daneben die zugehörige IP-Adresse und, sofern vorhanden, auch der Rechnername.



Bild 3.7: *Visual Traceroute* zeigt die Route zum Zielrechner auf der Karte an

Aber Moment, da steht noch mehr: Diese App nutzt *Maxminds GeoIP*-Datenbank um festzustellen, wo sich die entsprechenden IP-Adressen befinden. So kann sie die Standorte auf der Karte anzeigen und auch in der Liste benennen. Dazwischen in Grün und auf dem Screenshot etwas schwer erkennbar, die Zeit, die das anfragende Datenpaket für den Weg dorthin und zurück (daher „Roundtrip“, was soviel wie „Rundreise“ heißt) benötigt hat.

Da diese App allerdings leider aus dem Playstore verschwunden ist, sei auf die ähnliche App namens **Visual Tracert** verwiesen. Diese kann die angezeigten Routen sogar als KML-Datei für Google Maps und Google Earth exportieren.



Visual Tracert

Jetzt wissen wir also, dass der Server erreichbar ist. Von einem anderen Rechner aus ließe sich noch feststellen, ob jemand (vielleicht ein Freund, der gerade am PC sitzt) auch auf den gewünschten Service zugreifen kann. Warum können wir das dann nicht?

Antwort auf diese Frage könnte u. a. **MobiPerf** (Bild 3.8) geben. Neben umfangreichen Informationen zur Konfiguration unseres Androiden und seines Netzwerks kann diese App nämlich auch feststellen, welche Dienste der Netzwerk-Anbieter ggf. gesperrt hat. So zeigt das Beispiel des Screenshots, dass der SMTP-Port 25 nicht genutzt werden kann – hier ist es also auf normale Weise nicht möglich, eine Mail zu verschicken.



MobiPerf



Bild 3.8: Mit **MobiPerf** lässt sich u. a. feststellen, welche Ports ggf. gesperrt sind

Mit dieser App lassen sich beispielsweise auch die Latenzzeiten für DNS-Lookup/Ping/Verbindungsaufbau, die Bandbreite für Up-/Downloads, die Signalstärke und mehr ermitteln. Alle Testergebnisse werden dabei im Cache aufbewahrt. Damit lassen sie sich einerseits auch offline auslesen, andererseits aber ebenso mit späteren/früheren Ergebnissen (oder solchen unterschiedlicher Standorte) vergleichen.

Als recht praktisch dürfte sich auch **Net Status** (Bild 3.9) erweisen. Bei dieser App handelt es sich um eine kleine Toolbox, in der u. a. folgendes versammelt ist: Ping, Netstat, Arp-Table und der Scan eines angegebenen Netzwerk-Bereiches zum Auffinden möglicher „Nachbarn“. Auch die Netzwerk-Konfiguration des eigenen Gerätes lässt sich anzeigen.



Net Status

Bild 3.9: ping, netstat und mehr sind in der App **Net Status** versammelt

Träges Netz

Sind alle netzwerkabhängigen Apps durch die Bank grottig langsam, liegt dies sicher weniger an allen zuständigen Servern, sondern vermutlich eher an der eigenen Netzverbindung, beziehungsweise an der Netzversorgung des Anbieters. Doch wie lässt sich so etwas belegen?



Speedtest.net
Mobile

Eine mögliche Antwort ist auf Bild 3.10 zu sehen und nennt sich **Speedtest.net Mobile**. Die App eignet sich, um Schwachstellen beim Provider aufzudecken: Die Resultate periodischer Tests werden gespeichert, sodass man im Nachhinein eine Vergleichsmöglichkeit hat. Auf diese Weise ist leicht erkennbar, wo die lahme Ente sitzt und wo hingegen „Schmitts Katze“ abgeht.



Bild 3.10: Speedtest.net Mobile ermittelt den Datendurchsatz

Wird hingegen ein echter Benchmark-Test gewünscht, greift man beispielsweise zur abgebildeten App **cnlab SpeedTest**. Mit dieser lassen sich Messreihen erstellen, die man auch mit Referenzsystemen vergleichen kann. Allerdings erfolgt die Messung hier nicht „nebenbei“, sondern es wird separater Datentransfer verursacht: Pro Messung sind dies laut der App-Beschreibung bis zu 7MB.



cnlab SpeedTest

Bild 3.11: Mit **cnlab SpeedTest** lassen sich Messreihen erstellen

Wer verbrät mein Datenvolumen?

Wer bereits Android 4.x (4.0 aka *Ice-Cream-Sandwich*, 4.1 aka *Jelly Bean*) auf seinem Gerät laufen hat, kann diese Frage recht einfach beantworten, denn hier ist die entsprechende Funktionalität bereits von Haus aus im System integriert: Eine Überwachung des Datenverbrauchs bis auf App-Ebene herab (sogar getrennt nach Verbrauch bei Vorder- und Hintergrundaktivität) mit Statistik-Graph und einschließlich der Möglichkeit zum Festlegen eines Warn- und eines „harten“ Limits (siehe Bild 3.12), natürlich getrennt nach WLAN und mobiler Datenverbindung.



Bild 3.12: Android-Systemeinstellungen: Datenverbrauch im Blick ab Android 4.0



3G Watchdog

Doch auch für den Großteil der Android-Nutzer, die noch nicht in den Genuss dieser Versionen gekommen sind, sind Hopfen und Malz noch lange nicht verloren, denn für sie gibt es Apps wie beispielsweise **3G Watchdog** (Bild 3.13). Diese App überwacht die mobile Datenverbindung (3G/Edge/GPRS) und deren Trafficverbrauch, zeigt ein Benachrichtigungssymbol (Grün, Orange, Rot) in der Statuszeile und gibt eine detaillierte Übersicht zum Verbrauch. Zwei Widgets stehen auch zur Wahl.

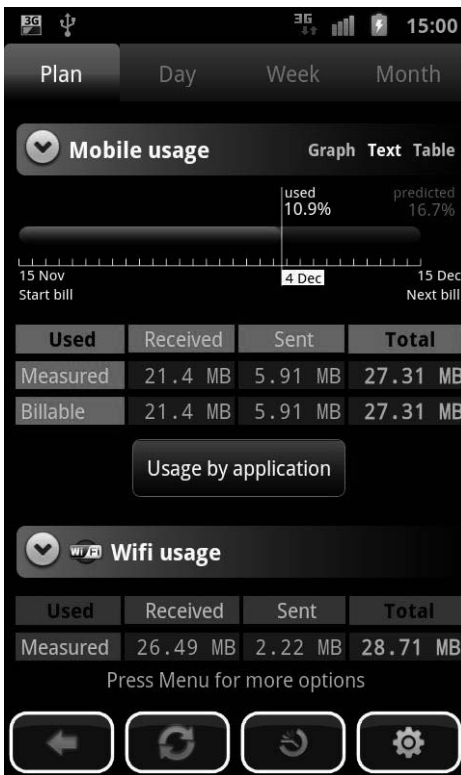


Bild 3.13: 3G Watchdog überwacht mobile Datenverbindungen

Aber 3G Watchdog kann noch mehr. Sicher: Es warnt vor und bei Erreichen der konfigurierten Limits – was für sich genommen schon eine gute Sache ist. So richtig interessant wird es, wenn außerdem die App **APNdroid** installiert ist: Kurz vor Erreichen des eingestellten Limits dreht 3G Watchdog dann nämlich einfach den Hahn zu! Der Zugangspunkt (in der Android-Konfiguration) wird dazu von **APNdroid** so verändert, dass er nicht mehr funktioniert. Und bevor jetzt Panik ausbricht: Selbstverständlich lässt sich diese Änderung rückgängig machen.



APNdroid

Ist das zu überwachende Gerät mit einem root-Zugang versehen, lassen sich an dieser Stelle u. U. auch zwei Fliegen mit einer Klappe schlagen: Bereits im Abschnitt 1.2 unter *Permissions überwachen* wurde die App **LBE Privacy Guard** vorgestellt. Diese kann mehr als nur die Zugriffe auf bestimmte Berechtigungen überwachen – nämlich auch den Datenverbrauch. Nebenbei lässt sie sich auch gleich als Firewall einsetzen, um bestimmten Apps den Netzzugriff generell zu verbieten – oder ihn wahlweise auf WLAN bzw. das mobile Datennetz zu beschränken – wie in Bild 3.14 ersichtlich.



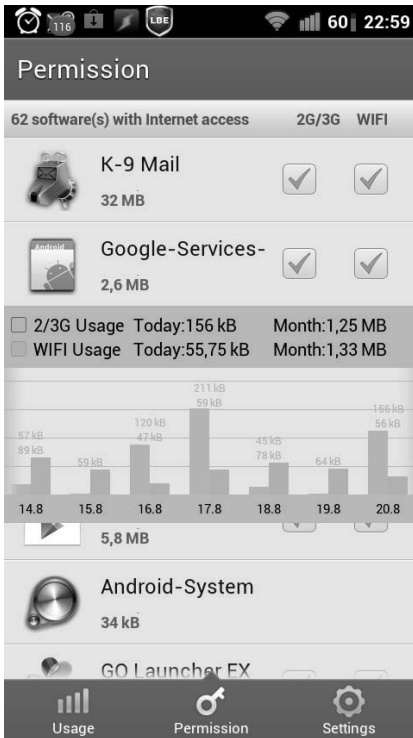


Bild 3.14: Auch **LBE Privacy Guard** hat einen Datenmonitor an Bord

Remote-Laufwerke mounten

Sicher gibt es eine Reihe guter **Datei-Manager**, mit denen man auf's Netzwerk zugreifen kann. Doch spätestens wenn es um das Abspielen von Titeln aus einer größeren Video-Sammlung geht, wird das mühsam: Warum erst jede Datei händisch auf den Androiden kopieren? Geht das nicht einfacher?

Die erste Antwort wäre wahrscheinlich „Streaming“ – was jedoch in der Regel eine passende Streaming-Server-Software auf der Gegenseite voraussetzt. Viel praktischer wäre es doch, man hätte das entfernte Laufwerk lokal zur Verfügung!



CifsManager

Exakt das verspricht zum Beispiel der **CifsManager**. Der Name der App deutet es bereits an: Dieser Manager kümmert sich um den **Samba**-Netzwerkdienst, auch als „CIFS“ oder „Windows-Freigabe“ bekannt. Einmal konfiguriert, lassen sich so Freigaben auf „Knopfdruck“ einbinden und auch wieder entfernen. Und diese Freigaben können sich durchaus auf unterschiedlichen Maschinen befinden – die selbstverständlich über das Netz erreichbar sein müssen (natürlich über das entsprechende Netzwerk-Protokoll).



Bild 3.15: *CifsManager* kümmert sich um Samba- und Windows-Freigaben

Das Ein- und Aushängen der Laufwerke erfolgt hier manuell: Der Nutzer muss sich also selbst darum kümmern. Zwar handelt es sich dabei, nach einmaliger Einrichtung der „Laufwerke“, nur um wenige „Taps“ – doch naturgemäß ist der Anwender faul und möchte selbst das noch vereinfachen. Oder man möchte auf einen Linux/Unix-Server per NFS zugreifen.

Die Antwort auf die im Raum stehende Frage heißt **Mount Manager**, ist in Bild 3.16 abgebildet und kostet in Vollausstattung ein wenig mehr als zwei Euro. Dafür bringt er aber auch allerhand an Funktionalität mit: Neben Samba/CIFS wird, wie schon erwähnt, auch **NFS** unterstützt. Einen Kernel mit Unterstützung für „loadable modules“ und weitere Module vorausgesetzt, wären auch weitere Dateisysteme denkbar. Laufwerke werden bei Einschalten von WLAN aktiviert, sobald man sich im betreffenden Netz befindet. Gleiches gilt für den Start des Gerätes, Tasker-Support, Speicherplatz-Anzeige und mehr.



Mount Manager



Bild 3.16: *Mount Manager* unterstützt zusätzlich auch NFS

3.3 Sichere Übertragung

Für harmloses Surfen, ein paar News lesen und ähnliche Dinge muss man sich über sichere Übertragungswege sicher nicht den Kopf zerbrechen. Anders sieht es aus, wenn sensible Daten ins Spiel kommen: Betriebsgeheimnisse, Finanzdaten, neueste Entwicklungen oder auch nur die privaten Zugangsdaten zu irgendetwas. Beim Gedanken, dass da jemand mitlesen könnte, macht sich beim Anwender ein mulmiges Gefühl breit.

Dafür muss eine Lösung her. Lässt sich Android tauglich machen für „corporate use“?

Proxy, Tunnel & Co

Manchmal scheint es, als wäre „Gefühl alles“ und Namen nur „Schall und Rauch“, wie Doktor Faust sich so trefflich auszudrücken wusste (Faust I, Marthens Garten). Ist ein Proxy nun eine Art spezieller Tunnel – oder nutzt ein Tunnel eine spezielle Art von Proxy?



SSH Tunnel

Praktisch gesehen, haben beide viel gemeinsam, und so mancher Anwender weiß die beiden nicht recht auseinander zu halten. Manchem Entwickler geht es offenbar ähnlich. So liest man beispielsweise in der Beschreibung der App **SSH Tunnel**, die sich in erster Linie an hinter der Firewall befindliche Anwender zur Überwindung derselbigen richtet, dass es als „globaler Proxy“ fungieren kann.

Gemeinsam ist beiden auf jeden Fall eines: Sie sind oftmals gleichermaßen geeignet, gewisse Sperren zu umgehen. So möchten viele Firmen gern vermeiden, dass ihre Angestellten sich auf dubiosen Webseiten ihre Arbeitszeit vertreiben und haben daher die für das Web-Surfing i. d. R. zuständigen Ports 80 und 443 gesperrt. Der Zugriff muss stattdessen über einen im Haus befindlichen Proxy-Server (der als Vermittler fungiert und als einziger auf den genannten Ports „rauswählen“ darf) erfolgen. Natürlich ist auch Port 22 gesperrt, damit sich niemand auf fremde SSH-Server verbindet. Und auf dem Proxy sind wiederum eine ganze Reihe interessanter Webseiten gesperrt. Meister Schlauberger umgeht dies nun, indem er sich einen Tunnel baut: Daheim lauscht ein SSH-Server auf Port 443, und dahinter ist der Weg frei. Da Port 443 vom Firmen-Proxy für sichere (und verschlüsselte) Web-Verbindungen akzeptiert wird, lässt er unseren Meister Schlauberger brav durch ...

Und wie geht man das Ganze nun unter Android an?

Proxies

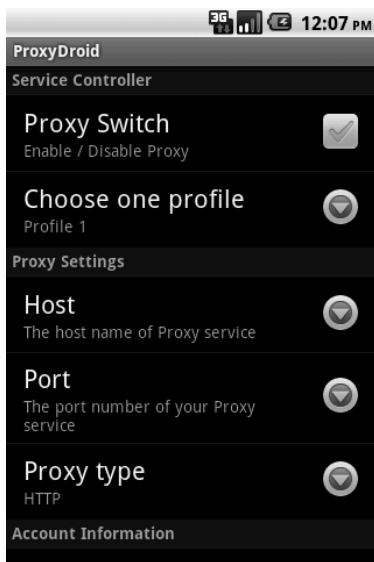
Grundlegende Proxy-Einstellungen sind unter Android vorhanden – nur nicht immer für den Anwender zugänglich. Fehlt der entsprechende Menüpunkt, lässt er sich mit **HTTP Proxy-Settings** dennoch öffnen.



Wem diese Grundfunktionalität nicht ausreicht, der greift beispielsweise zu **ProxyDroid** (Bild 3.17). Diese App will helfen, mit allen Apps auf dem Androiden auch über Proxies auf das Internet zuzugreifen (benötigt dazu allerdings *root*). Dies ist z. B. häufig in Firmen nötig, wo eine Firewall den direkten Zugriff unterbindet. *ProxyDroid* unterstützt dabei HTTP- / SOCKS4- / SOCKS5- Proxies, basic- / NTLM- / NTLMv2- Authentication, verschiedene Profile und mehr. Es lässt sich auswählen, welche Apps bei ihrem Zugriff auf das Internet über den Proxy geleitet werden sollen. Auch lässt sich ein konfigurierter Proxy für die Verwendung in einem bestimmten Netz (WLAN SSID / Mobiles Netzwerk) einschränken sowie bei Verfügbarkeit eines bestimmten Netzwerks automatisch aktivieren. Widgets ermöglichen ferner die schnelle (De-)Aktivierung von Proxies, und man kann sich per Klingelton und/oder Vibration sogar über Änderungen des Verbindungsstatus informieren lassen. Damit ist doch eigentlich an alles gedacht, oder?



HTTP Proxy
Settings



ProxyDroid

Bild 3.17: *ProxyDroid* ist ein vielseitiger Proxy

Wenn das Wörtchen „eigentlich“ nicht wäre. Denn zumindest einen weiteren Punkt gäbe es noch: Anonymität. Ein Synonym in der Netzwerk-Landschaft dafür wäre **TOR** – der anonymisierende Routing-Dienst. Und damit kommt **Orbot** (Bild 3.18) ins Spiel, der offizielle Android-Port von **TOR** für Android. Mit dieser App wird der Traffic anonymisiert – der Absender eines Netzwerk-Paketes ist also beim Empfänger nicht mehr erkennbar. Unter Android 2.x funktioniert das laut Beschreibung mit Firefox und dem ProxyMob-Add-on, mit **Orweb: Proxy+Privacy Browser** sowie mit Orbot-enabled Apps wie **Gibberbot** (secure chat). Transparenter Proxy-Support soll auf den meisten gerooteten Geräten verfügbar

sein. Unter Zuhilfenahme anderer Apps (wie dem bereits genannten *HTTP Proxy Settings*) soll es wohl auch mit anderen Apps funktionieren. Allerdings könnte dieser Zusatzaufwand mittlerweile obsolet sein: Ein aktueller Screenshot (siehe Bild 3.18) legt nahe, dass *Orbot* sich mittlerweile selbstständig sämtlichen anderen Anwendungen zur Verfügung stellen kann.



Orweb: Proxy+Privacy
Browser



Orbot



Gibberbot

Bild 3.18: Orbot bietet Zugriff
auf das anonymisierende TOR-Netzwerk

Tunnel

Alles zappenduster? Oder was für ein Tunnel? Manchmal gibt es keinen direkten Weg, und man muss Zwischenstation machen. Von A nach C geht es dann nur über B. Und das nennt sich **Tunnel**: „über B nach C“. Stark vereinfacht ausgedrückt, denn häufig kommt hinzu, dass man dazu in einen speziellen „Schutzanzug“ muss. In der Regel hat das auch etwas mit Datensicherheit zu tun und meistens auch mit SSH.

Als erste Wahl zu diesem Thema wäre sicherlich **ConnectBot** zu nennen. Bei der App handelt es sich um eine einfache, mächtige, Open-source-SSH-Client-Anwendung, die es ermöglicht, mehrere simultane SSH-Sessions zu betreiben, sichere Tunnel aufzubauen (ah!) und mehr – sogar Copy und Paste zwischen Anwendungen wird unterstützt. So kann man auch „mal eben kurz“ auf die Kommandozeile des Linux/Unix Servers zugreifen, der am anderen Ende der Welt steht.

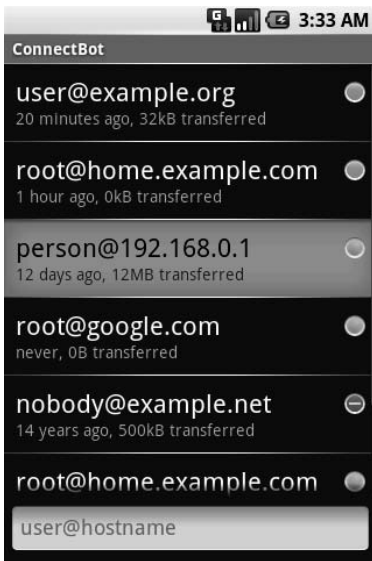


Bild 3.19: *ConnectBot* ist ein SSH-Client, der sich auch aufs Tunneln versteht

Da sich die Einrichtung eines sicheren Tunnels ohne Vorkenntnisse nicht so ganz trivial gestaltet, und auch ganz allgemein die ersten Schritte so manchen Anwender vor das eine oder andere Problem stellen könnten, sei hier noch auf ein paar Artikel im Netz verwiesen:

- **Verwendung von SSH-Keys mit ConnectBot**



<http://www.dev-etho.de/public-key-authorisierung-mit-android-und-connectbot/>

- **SSH-Tunnel mit ConnectBot und ProxyDroid**



<http://www.ignitoe.de/index.php/2011/05/android-ssh-tunnel-hotspot-surfen-sichern/>

- **ConnectBot Basic Features** (YouTube-Video)



<http://www.youtube.com/watch?v=3mPNL3dBsns>

Weitere Kandidaten (sowohl für den Tunnel als auch zum Thema Proxy) finden sich in der Übersicht bei AndroidPIT.



<http://www.androidpit.de/de/android/forum/thread/436826/>

AdBlock

Oh, ich höre schon das Geschrei: „Die armen Programmierer, die am Hungertuch nagen müssen ...“

Damit mich keiner falsch versteht: Ich möchte niemandem die Butter vom Brot nehmen (die Wurst schon gleich gar nicht). Ebenso wenig soll dies ein Aufruf zur kompletten Reklame-Blockierung sein. Aber es gibt hin und wieder durchaus berechtigte Gründe, warum ein solcher „Ad-Blocker“ ans Werk gehen soll. Beispiele gefällig? Oh, „fällig“ ist da richtig gut: Abo-Fallen. Erwachsene sollten dank vollständig aktualisiertem und mit allen nötigen Zusatz-Modulen versehenem GMV halbwegs darauf achten können, wo sie hintippen. Von einem Kind zum Beispiel, dem der Androide „eben einmal für ein Spiel“ überlassen wird, kann man dies hingegen nicht unbedingt erwarten.

Dann wären da ja auch noch die ganzen Web-Bugs und andere Tracker, die gern das Nutzer-Verhalten protokollieren wollen. Natürlich nur zu unserem Besten, versteht sich (gemeint ist damit jedoch, dass sie uns „zum Besten halten“ wollen). Spätestens hier geht es dann aber wieder um „Datenschutz“ und „Privatsphäre“ und damit wird es Ernst.

Zum Glück gibt es einige Möglichkeiten, sich zu wehren. Diese benötigen jedoch fast ausnahmslos *root*.



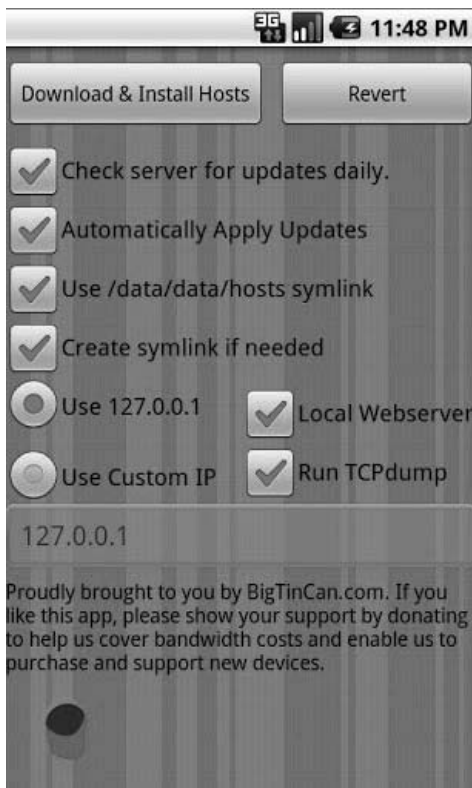
Am bekanntesten ist sicherlich **AdFree Android**. Diese App ersetzt die Hosts-Datei mit einer Version, in der die meisten bekannten Ad-Server ins Daten-Nirvana geschickt

werden, indem ihnen eine „leere“ IP-Adresse zugewiesen wird. Dies blockt Werbe-Zugriffe effektiv – nicht nur im Browser, sondern in allen Apps.

(Hinweis: Zur Wiederherstellung des Ursprungs-Zustandes nicht einfach die App deinstallieren, sondern vorher mit Hilfe der App die ursprüngliche Host-Datei wieder herstellen („Revert“). *AdFree* macht ja nichts weiter als diese Datei einmalig (oder einmal täglich) anzulegen – die Filterung der entsprechenden Netzzugriffe erledigt das Android-System anschließend selbst!)



<http://www.androidpit.de/de/android/forum/thread/436855/Uebersicht-Netzwerk-AdBlocker>



AdFree Android

Bild 3.20: *AdFree Android* ist einer der beliebtesten Ad-Blocker

Ohne *root* kommt hingegen *AD Blocker & Net Toggle* (Bild 3.21) aus. Mit einem ganz einfachen Trick: Für die ausgewählten Apps gilt einfach die Regel, dass bei ihrem Start das Netzwerk deaktiviert wird. 100% effektiv. Auf Webseiten wird dabei dummerweise nicht nur die Werbung geblockt (was natürlich auch für andere Apps gilt, die außer Werbung noch andere Dinge im Internet zu tun haben).



AD Blocker & Net Toggle



Bild 3.21: *AD Blocker & Net Toggle* schaltet einfach das Netz aus – keine Werbung (aber auch sonst nichts)



AdBlock

Geht es lediglich um die Werbung im Browser, gibt es für den einen oder anderen ein passendes AddOn. Für beliebige Browser hingegen greift **AdBlock** (Bild 3.23), und zwar nach einem bereits *vorher* erklärten Prinzip: Die App arbeitet als Proxy und muss dem System daher als solcher bekannt gemacht werden. Wie letzteres funktioniert, wurde ja bereits beschrieben. Auch diese Variante kommt ohne *root* aus – sollte also für jeden Androidler nutzbar sein.

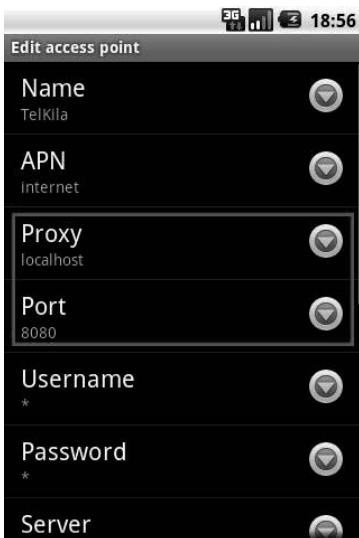


Bild 3.22: *AdBlock* geht das Problem an, indem es sich als Proxy vor den Browser schaltet



Eine weitere Variante wurde bereits beim Thema **Firewalls** genannt: Mit einer Firewall ließe sich der Netzzugang einzelner Apps unterbinden. Eine komplexe Firewall könnte auch für bestimmte Apps lediglich bestimmte Ziele sperren. Dies würde jedoch auch eine komplexe Benutzer-Oberfläche erfordern, weshalb sich wohl noch niemand dieser Aufgabe gewidmet hat. Technisch versierte Anwender greifen daher bei Bedarf zu einer Terminal-App und verwenden das *iptables*-Binary direkt. Das setzt natürlich eine genaue Kenntnis der Syntax voraus.

3.4 WLAN

Netzwerk und Android – da ist WLAN sicher ein zentrales Thema. Und so soll sich dieses Kapitel einigen WLAN-spezifischen Dingen widmen.

VPN

Ein VPN ist eigentlich so etwas wie ein „systemweiter Tunnel“, mit dem der Client (in unserem Fall der Androide) sich in das Netzwerk des Servers einbindet, als wäre er direkt dort vor Ort. Ich bin also zu Hause, und mein Androide ist im Office der Firma – obwohl ich ihn in der Hand halte.

Eine Angelegenheit, die besonders im Unternehmens-Umfeld (und dort speziell für Außendienst-Mitarbeiter) interessant ist, wo man gewisse Dienste nur im **IntraNet** bereit hält. Was sich aber gut auf den Privatbereich übertragen lässt: Auch im heimischen Netz gibt es einiges, das nicht unbedingt der Öffentlichkeit zur Verfügung stehen soll, das man aber dennoch selbst von unterwegs verfügbar haben möchte. Etwa das Web-Interface des eigenen Routers, die Drucker oder die Photosammlung. Welche Helferlein uns zum Thema VPN zur Verfügung stehen, zeigt die Übersicht bei AndroidPIT auf.



<http://www.androidpit.de/de/android/forum/thread/436786/>

Android bringt bereits von Haus aus einen VPN-Client mit, der auch mit den meisten VPN-Servern kompatibel ist. Trifft letzteres nicht zu, sind oft tiefer greifende Maßnahmen nötig, da die nötigen Tools der Drittanbieter in der Regel *root* voraussetzen. Aus diesem Grund wird der vorinstallierte Client als „erste Wahl“ angesehen: Ein super sicherer Spezial-VPN-Server erhöht die Sicherheit schließlich nicht, wenn im Gegenzug sämtliche mobilen Teilnehmer ihre Geräte rooten müssen.

Die Einrichtung eines VPN mit Android-Bordmitteln beschreibt ein Artikel bei TECChannel.DE im Detail. Wie in bereits genannter Übersicht, wird auch dort auf die Verwendung von **VPN Show** hin-



http://www.tecchannel.de/kommunikation/handy_pda/2033962/smartphone_android_praxis_vpn_einrichten_und_nutzen/



VPN Show

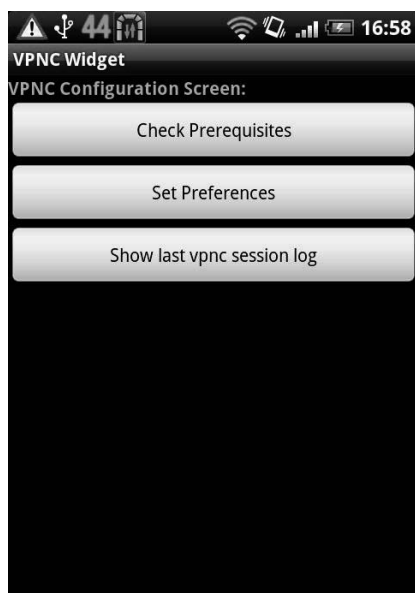
gewiesen, das einen Schnellzugriff auf die im Gerät vorhandenen VPN-Einstellungen bereitstellt.

Server von z. B. SonicWALL oder Cisco (Support für Cisco wurde erst mit Android 4.0 aka Ice Cream Sandwich integriert) verhalten sich jedoch nicht immer kompatibel zu den VPN-Standards PPTP bzw. L2TP. Stattdessen stellen deren Anbieter eigene Android-Apps zur Einrichtung der VPN-Verbindung zur Verfügung, die jedoch *root* voraussetzen.



VPNC Widget

Ähnlich sieht es auch bei der Fritz!Box aus. Die leicht peinliche Aussage von AVM zum Thema lautet: *Für Apple iOS-Geräte ist die Nutzung per VPN aber grundsätzlich möglich. Eine VPN-Verbindung von Google Android zur FRITZ!Box wird hingegen nicht unterstützt.* Apfel ja, Android nein. Was AVM nicht unterstützt, tun dafür andere: Mit dem **VPNC Widget** (Bild 3.23) lässt sich ein Zugang schließlich doch realisieren – *root* und ein paar andere „Kleinigkeiten“, die in der Beschreibung der App erklärt werden, vorausgesetzt. Ein „Patchen“ der App, wie in einigen Anleitungen beschrieben, ist hingegen nicht mehr nötig.



<http://www.nodch.de/sicherer-netzwerkzugriff-mit-openvpn-und-android/2989/>

Bild 3.23: Dank *root* und **VPNC Widget** klappt es auch mit der Fritz!Box

Eine Alternative scheint für einige Anwender *OpenVPN* zu sein – zumal die entsprechende App bei einigen Custom-ROMs bereits vorinstalliert ist. Eine Anleitung für die Konfiguration unter Android findet sich bei **Nodch.DE**, für den notwendigen Server ist natürlich ebenfalls Sorge zu tragen.

Eine echte Alternative für viele Anwender hingegen könnte **NeoRouter** (Bild 3.24) darstellen: All die lästigen Voraussetzungen wie *root*, separates Kernel-Modul und aufwendige Installation scheinen bei dieser Lösung zu entfallen. Auf der Homepage werden Software-Pakete für alle möglichen Systeme (darunter Linux, Mac, BSD, Windows) angeboten, damit auch die Gegenstelle versorgt ist. Das Ganze verspricht eine einfache Umsetzung („einfacher als OpenVPN und schneller als LogMeIn Ignition“). Für den Einsatz im Unternehmensumfeld steht eine stabile, für Version-Junkies eine häufig aktualisierte Version zur Verfügung. Beide sind gratis.



NeoRouter



Bild 3.24: **NeoRouter** verspricht: „einfacher als **OpenVPN** und schneller als **LogMeIn Ignition**“

Zum Thema „Unterstützung für Fritz!Boxen“ hat sich Neo allerdings nicht geäußert.

Automatische (De-)Aktivierung

Mit diesem Thema greifen wir dem vierten Teil des Buches (*Tuning*) bereits ein wenig vor: Da WLAN bereits im Standby-Betrieb einen nicht unbedeutenden Stromverbrauch aufweist (etwa das Zwanzigfache des GPS-Standby – was aber nur ca. 3% des Verbrauches eines auf niedrigste Stufe eingestellten Displays ausmacht), ist ein Abschalten bei fehlendem Bedarf sicher keine verkehrte Idee. Natürlich ließe sich das manuell erledigen, doch



<http://www.androidpit.de/de/android/forum/thread/429837/>

vergesslich wie wir sind, überlassen wir das besser nicht dem Zufall. Eine Übersicht verfügbarer Werkzeuge für diesen Zweck findet sich natürlich wieder im Forum.

Die einfachste Variante lässt sich mit Bordmitteln regeln und nennt sich „WLAN-Standby-Richtlinie“. Mittels dieser lässt sich WLAN abschalten, wenn man das Display abschaltet. Oder auch nicht. Oder auch nur dann, wenn kein Ladekabel angeschlossen ist. Für manchen Anwender mag das bereits genügen – doch hat es durchaus auch den einen oder anderen Haken: etwa wenn man im Hintergrund Musik von einem Server streamt oder periodisch Daten synchronisieren möchte (was dann wohl über das mobile Netzwerk erfolgen würde). Für diese und ähnliche Fälle muss also eine Alternative her.

Die könnte beispielsweise **WiFi Location Toggle** heißen und ist in Bild 3.25 zu sehen. Mit dieser App lässt sich festlegen, an welchen Orten man WLAN benutzen möchte: Betritt man die definierten Zonen, wird WLAN aktiviert – verlässt man sie, wird es wieder abgeschaltet. Wer bereits *Tasker* im Einsatz hat, kann auf diese App natürlich verzichten und setzt das dort mit entsprechenden Profilen um. Zumal *WiFi Location Toggle* auf fünf Standorte begrenzt ist.

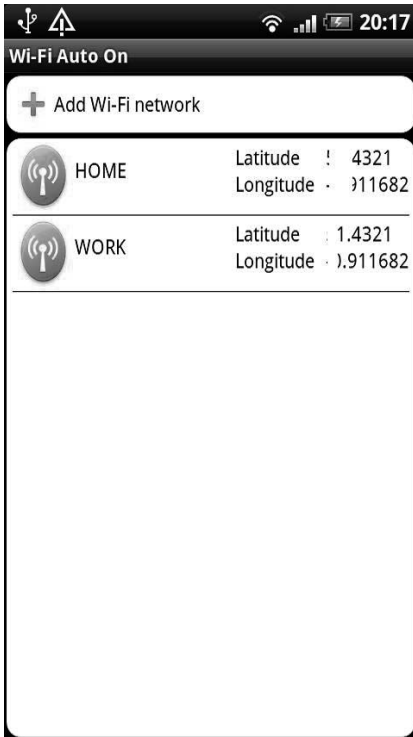


WiFi Location
Toggle

Bild 3.25: *WiFi Location Toggle* schaltet das WLAN automatisch an konfigurierten Orten ein

Schon ganz clever. Dabei ist natürlich bereits ein größerer Bereich abgedeckt als vielleicht nötig – denn wer weiß schon so genau, wie weit das WLAN-Signal reicht, welcher Radius

dafür definiert werden muss? Diesen Überlegungen muss man sich bei Verwendung von **WiFi Auto On** (Bild 3.26) nicht stellen. Hier werden einfach die gewünschten Netzwerke definiert und um den Rest kümmert sich die App selbst.



WiFi Auto On

Bild 3.26: *WiFi Auto On* ermittelt die Orte selber anhand der konfigurierten WLAN-Netze

Aber woher wissen diese Apps denn nun, wann man sich im fraglichen Bereich aufhält? Würden sie dafür GPS verwenden, fiele der Stromverbrauch ja noch höher aus. Keine Sorge: Das tun sie nicht. Stattdessen merken sie sich die in der Nähe befindlichen Mobilfunkzellen. Und die spürt ein Mobiltelefon ohnehin auf, werden sie doch für die Telefonie-Funktion benötigt.

Zu suspect? Okay, es gibt auch noch andere Möglichkeiten. So fährt beispielsweise **Auto WiFi Toggle** (Bild 3.27) eine komplett andere Strategie. Vereinfacht gesagt, schaltet die App je nach Konfiguration ein aktiviertes WLAN entweder aus, wenn man mit keinem Netz verbunden ist, oder es schaltet WLAN von Zeit zu Zeit an und wartet kurz, ob eine Verbindung aufgebaut wird (andernfalls wird WLAN wieder deaktiviert). Das ist aber nur die einfache Fassung. Alles lässt sich bis ins Kleinste konfigurieren. So kann z. B. das Prüfintervall nicht nur global festgelegt werden, sondern für einzelne Zeiträume unterschiedlich.



Auto WiFi Toggle

Das ist ja auch sinnvoll: Wer weiß, dass er generell zwischen Mitternacht und sechs Uhr morgens schläft, braucht in der Zeit ja nicht so oft auf verfügbares WLAN prüfen.



Bild 3.27: *Auto WiFi Toggle* prüft in Intervallen, ob sich bekannte WLAN-Netzwerke in der Nähe befinden



Battery Saver

Wer wirklich alle Register ziehen will, kann auch zu **Battery Saver** (Bild 3.28) greifen. Womit wir definitiv in den vierten Teil des Buches eingreifen, denn diese App befasst sich nicht nur mit WLAN, sondern nebenbei auch gleich mit Bluetooth und GPS. Sie kümmert sich u. a. um die Stärke des WLAN-Signals, aber ebenso um das Zellen-Signal und anderes und reagiert auf konfigurierte Schwellwerte. Sie schaltet die entsprechenden Dinge selbsttätig aus, sobald die Grenzwerte unterschritten werden: Reicht die Signalstärke nicht mehr aus, zum Beispiel in der U-Bahn einiger Großstädte, hat es ja auch keinen Sinn. Wie viel zusätzliche Akku-Laufzeit sich damit „herauskitzeln“ lässt, hängt von verschiedenen Kriterien ab und ist daher eher ein recht individueller Wert. Auch die Playstore-Kommentare sind da wenig aufschlussreich.



Bild 3.28: *Battery Saver* kümmert sich bei Bedarf auch um Bluetooth und das Funknetzwerk

Tethering

Da ist man also unterwegs und würde gern mal schnell mit dem Tablet oder dem Notebook ins Netz der Netze. Natürlich kein WLAN weit und breit – zumindest keines, dem man traut. Da bietet sich doch das mobile Datennetz des Android-Telefons an, oder? Klar, mit Android 2.2 oder neuer gar kein Thema, da erstellt man sich einfach seinen eigenen Hotspot. Ist ja von Haus aus dabei.

Die zugehörigen Einstellungen finden sich unter *Einstellungen* → *Drahtlos & Netzwerke* → *Tethering & mobiler Hotspot*. Je nach Android-Version (und teilweise auch Geräte-Hersteller) heißt dieser Punkt u. U. leicht anders und bietet auch unterschiedliche Möglichkeiten. So kann eventuell zusätzlich zum WLAN-Tethering auch noch USB-Tethering im Angebot sein.



Bild 3.29: Android-Systemeinstellungen: *WLAN-Hotspot einrichten*

Die Einrichtung ähnelt der eines Routers – was ganz logisch ist, denn schließlich möchte man seinen Androiden ja gerade in einen solchen verwandeln. Dazu müssen zunächst einige wenige Daten festgelegt werden, wie auf dem Screenshot erkennbar: die zu verwendende SSID für das zu errichtende drahtlose Netzwerk, die Sicherheitsstufe („offen“ und WPA2“ stehen dafür i. d. R. zur Auswahl) sowie ggf. ein „Passwort“ (auch als „WLAN-Schlüssel“ bekannt). Ist das geschehen, lässt sich der „mobile Hotspot“ jederzeit aktivieren und deaktivieren.

Doch wie sieht es aus, wenn man eine ältere Android-Version verwendet oder der Hersteller das Tethering aus dem Menü entfernt hat? Dann erledigt das die App eines Drittanbieters, vorausgesetzt, man verfügt auf dem Androiden über *root*. Ohne diesen wird es zwar nicht unmöglich – aber zumindest schwierig und unbequem.

Die wohl beliebteste App in diesem Umfeld ist **Wireless Tether for Root Users** (Bild 3.30).

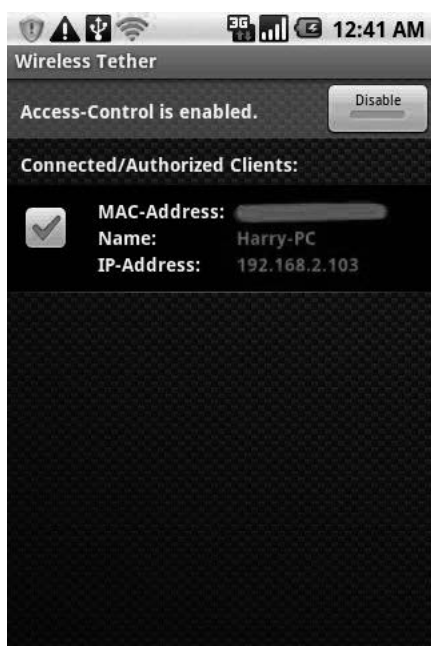


Bild 3.30: *Wireless Tether* benötigt root, funktioniert aber auch auf älteren Android-Versionen



Wireless Tether for Root Users

Eine wichtige Voraussetzung zu deren Nutzung ist bereits im Namen enthalten, hinzu kommt ein Kernel mit Netfilter-Support. Die meisten **Custom-ROMs** dürften beide Voraussetzungen erfüllen, während die vom Hersteller installierte Firmware selbst nach dem Rooten häufig den zweiten Punkt nicht erfüllt. Hat man diese Hürden jedoch erfolgreich gemeistert, steht das Internet per WLAN und Bluetooth bereit, in den meisten Fällen als AdHoc(Peer-to-Peer)-Netz, auf einigen Geräten



auch wie ein gewöhnlicher Hotspot im „Infrastructure“-Modus. Als Verschlüsselung kommen 128Bit WEP sowie auf einigen unterstützten Geräten auch WPA/WPA2 zum Einsatz. Als weitere Zugriffskontrolle steht (wie in Bild 3.30 zu sehen) ein MAC-Filter bereit: So lassen sich unliebsame „Gäste“ selbst dann aussperren, wenn sie irgendwie an den Netzwerkschlüssel gekommen sein sollten.

Wer an der genannten zweiten Voraussetzung (dem angepassten *Kernel*) scheitert, kann auf **Barnacle Wifi Tether** (Bild 3.31) ausweichen. *root* ist allerdings auch bei dieser App nötig, und auf den „Infrastructure“-Modus muss verzichtet werden, was aber in den meisten Fällen locker zu verschmerzen ist. Neben der SSID lässt sich bei *Barnacle* optional auch die BSSID einstellen, zur Verschlüsselung gesellt sich auch hier die Zugriffskontrolle per MAC-Filter. Zahlreiche weitere Konfigurationsmöglichkeiten geben dem Anwender die Möglichkeit, die App an seine Bedürfnisse anzupassen.



Barnacle WiFi
Tether

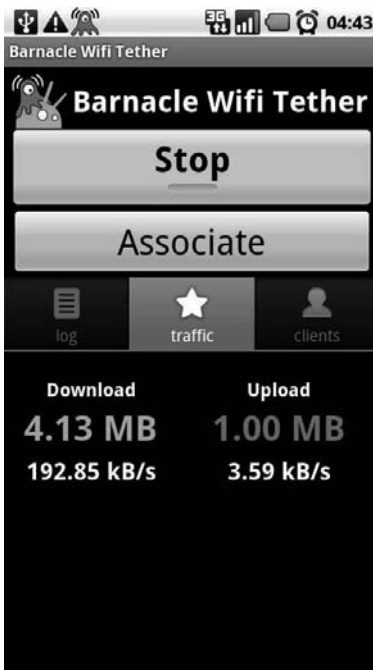
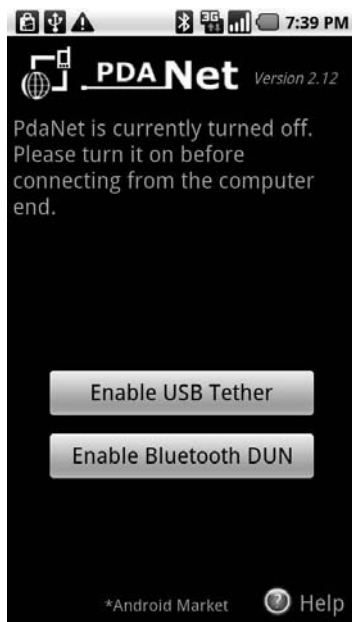


Bild 3.31: *Barnacle Wifi Tether* stellt eine alternative Lösung dar

Steht *root* nicht zur Verfügung, fällt WLAN als Möglichkeit wohl aus. Es kann jedoch auf **PdaNet** (Bild 3.32) ausgewichen werden, um das Netz zumindest per USB oder Bluetooth zur Verfügung stellen. Man muss die Dinge positiv sehen: Bei einem Kabel ist klar erkennbar, wer dran hängt, ein „heimliches Einklinken“ wird somit deutlich erschwert. Als nette Dreingabe gibt es dazu die Möglichkeit, vom PC aus SMS zu empfangen/senden.

Ist das Tethering einmal eingerichtet, könnte man es auf Knopfdruck aktivieren, wäre der Knopf nicht so versteckt, insbesondere bei den Bordmitteln. Abhilfe schaffen hier etliche Widgets für den Schnellzugriff, die teilweise das Schalten direkt übernehmen.



PdaNet

Bild 3.32: *PdaNet* stellt Tethering auch ohne root zur Verfügung – allerdings nur per USB-Kabel oder Bluetooth



Reverse Tether

Was passiert nun, wenn man das Ganze umdreht? Klar: Man bekommt den Laptop-Deckel nicht mehr auf. Unsinn: Gemeint ist natürlich eine Umkehr der Verbindungsrichtung, etwa wenn am aktuellen Standort nur kabelgebundenes Netzwerk zur Verfügung steht. Dann ließe sich die am Laptop bestehende Internet-Verbindung auch vom Androiden aus nutzen. Per USB-Kabel ermöglicht dies beispielsweise die App **Reverse Tether** (Bild 3.33). Sie unterstützt eine automatische Konfiguration, lässt aber auch manuelle Anpassungen zu. Vorausgesetzt, das Android-Gerät wird unterstützt (leider funktioniert die App nicht auf allen Geräten – hier scheint es hin und wieder zu Kompatibilitäts-Problemen zu kommen), steht die Internet-Verbindung pronto zur Verfügung. Alles, was es dazu braucht, ist ein USB-Kabel sowie ggf. (bei Einsatz von Windows) der entsprechende Geräte-Treiber für den Androiden. Optional kann man sich nun auch bei jedem Anstecken des USB-Kabels automatisch fragen lassen, ob die Internet-Verbindung hergestellt werden soll.



Reverse Tether



Bild 3.33: *Reverse Tether* ermöglicht „umgekehrtes Tethering“ via USB

Es gibt eine Gratis-Testversion, die allerdings hinsichtlich der Verbindungszeit eingeschränkt ist. Damit lässt sich jedoch auf jeden Fall feststellen, ob die App mit dem eigenen Gerät überhaupt funktioniert. Die Vollversion kann man sodann für knapp vier Euro erwerben.

Sollte diese App nicht mit dem Wunschgerät kompatibel sein, gibt es noch ein paar Alternativen. Diese bestehen jedoch nicht aus einer einfachen App, sondern bedürfen oftmals ein wenig Handarbeit (etwa das Anpassen von Systemdateien auf dem Androiden – wie der Datei `/system/bin/wpa_supplicant` zur Ermöglichung des Zugriffs auf Ad-Hoc-Netzwerke per WLAN). Oder sie sind auf ein bestimmtes Betriebssystem auf dem PC/Laptop angewiesen – wie im Falle von *Android Reverse Tethering for Windows users*.

Eine Methode, die sich einfach mit Hilfe einer Terminal-App umsetzen lassen sollte, beschreibt Rotemmiz in einem Beitrag bei StackExchange:

```
ifconfig wlan0 up
iwconfig mode auto
iwconfig wlan0 essid „your SSID“ channel 11 mode auto
fconfig wlan0 10.0.0.x netmask 255.255.255.0
```

Diese Zeilen gilt es natürlich als *root* auszuführen, wobei „your SSID“ durch die SSID des Access-Points und 10.0.0.x durch die für den Androiden zuständige IP-Adresse ersetzt werden müssen.



<http://forum.xda-developers.com/showthread.php?t=1371345>



<http://android.stackexchange.com/questions/19129/connect-android-phones-through-adhoc-wifi-network>



Eine weitere Möglichkeit beschreibt GWLlosa, ebenfalls bei StackExchange. In seinem Fall ermöglicht die manuelle Anpassung der Konfigurationsdatei `wpa_supplicant.conf` den Zugriff auf AdHoc-Netzwerke via WLAN. Glücklicherweise, wer in den erweiterten WLAN-Einstellungen, wie im Screenshot in Abschnitt 3.1 unter *WLAN-Konfiguration* zu sehen, den Kanal für „Peer-to-Peer-Verbindungen“ einstellen kann: Ein solches Gerät unterstützt den Ad-Hoc-Modus von Haus aus.

Wesentlich einfacher geht es, wenn der Laptop/PC ein vollwertiges „Infrastruktur“-WLAN (im Gegensatz zu „AdHoc“) bereitstellen kann oder man über einen passenden WLAN-Reiserouter (bereits für unter 50 Euro im Handel erhältlich) verfügt. Dann nutzt man das bereitgestellte WLAN nämlich einfach wie jeden anderen Hotspot auch.

Hotspots & WLAN-Finder

Unterwegs und insbesondere im Ausland, wo man auf teure Roaming-Kosten gern verzichtet, ist so mancher scharf auf ein verfügbares WLAN. Viele Hotels und mittlerweile auch Cafés bieten ihren Gästen auf Anfrage einen Zugang auf diese Weise an. Auch die Telekom hält etliche Hotspots bereit. Die Frage, die sich stellt, ist nur: Wie bzw. wo findet man diese Zugangspunkte?

Natürlich gäbe es da zunächst den in Android integrierten WLAN-Scan, der sich unter *Einstellungen* → *Drahtlos & Netzwerke* → *WLAN-Einstellungen* findet. Während sich dieser wunderbar eignet, so man das Netzwerk kennt, zu dem man sich verbinden will (also etwa das im eigenen Hotel, zu dem der Portier gerade die Zugangsdaten auf einem Kärtchen übergeben hat), tauchen die ersten Probleme spätestens auf, wenn kein WLAN angezeigt wird. Schon fünfzig Meter weiter könnte eines sein, nur in welcher Richtung? Und ist ein als „offen“ gekennzeichnetes WLAN auch wirklich „offen“ oder kommt man nach dem Verbindungsaufbau lediglich mit dem Browser auf eine Anmeldeseite?

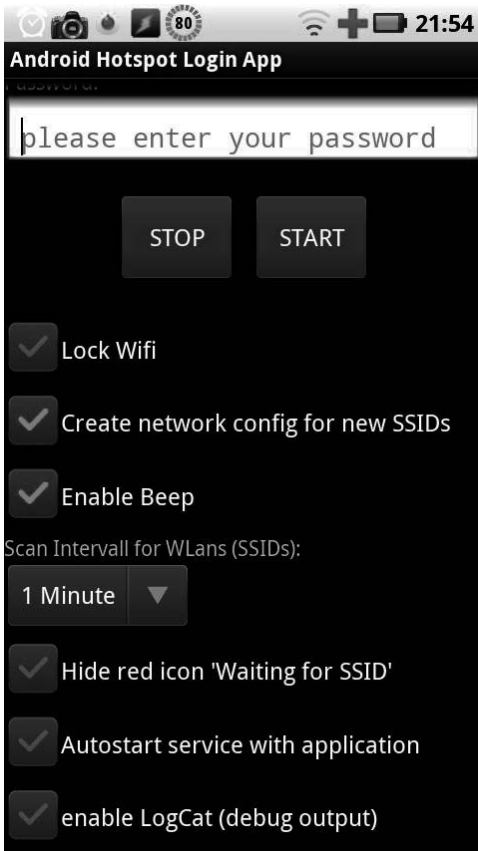


<http://www.androidpit.de/de/android/forum/thread/429837/>

Eine Übersicht im Forum bei AndroidPIT nennt eine Reihe von Tools, die genau diese Fragen beantworten wollen. So kann man beispielsweise Telekom-Hotspots relativ leicht aufspüren: Sie lassen sich an ihrer **SSID** erkennen. Da die zu verwendenden Zugangsdaten bei allen diesen Hotspots identisch sind, stünde einer automatischen Anmeldung eigentlich nichts im Weg. Zu dumm nur, dass diese jeweils nach dem Aufbau der (unverschlüsselten) WLAN-Verbindung über eine Webseite erfolgt.

Android Hotspot Login (Bild 3.34) erledigt dies dennoch ohne viel Schnick-Schnack: Einfach die Login-Daten konfigurieren, ggf. das Scan-Intervall anpassen und ein paar Häkchen umsetzen - fertig. Bei Bedarf jetzt den Service noch starten, und sobald ein passender Hotspot in der Nähe ist, verbindet die App automatisch, wobei es ggf. „Piep“ macht. So die Theorie. In der Praxis scheinen Änderungen seitens der Telekom

die Apps aus dem Tritt gebracht zu haben. Doch wenn ein nach September 2011 datiertes Update verfügbar werden sollte, lohnt sich ein Blick auf diese App mit Sicherheit.



Android Hotspot Login

Bild 3.34: *Android Hotspot Login* soll automatisch mit Hotspots verbinden

Die „originale App“ von der Telekom selbst müsste das Problem doch eigentlich lösen. Werfen wir daher einen Blick auf *HotSpot Login* (Bild 3.35): Diese App soll unabhängig von der SIM-Karte oder sogar ohne selbige funktionieren – das wäre doch eine prima Sache für Tablet-Nutzer! Also flugs mal auf mein Testgerät (ohne SIM) gezogen und geschaut. Das Ergebnis ist ernüchternd: Im heimischen WLAN angemeldet, findet die App in München ganze 0 Hotspots, davon 0 in der näheren Umgebung. Wie kann das sein? Beschreibung nochmal lesen: Aha, die Suche funktioniert nur, wenn man an einem Telekom-Hotspot angemeldet ist. Tolle Logik: Um einen Telekom-Hotspot zu finden, muss man in einem solchen angemeldet sein. Dann allerdings braucht man ihn ja eigentlich nicht mehr zu suchen ...



HotSpot Login



Bild 3.35: *HotSpot Login* ist die originale App der Telekom

Ich teste ein wenig weiter. Am Hauptbahnhof gibt es einen Telekom-Hotspot, der von der App auch sogleich entdeckt wird. Die Anmeldung erfolgt ohne Rückfrage, ob ich das überhaupt will – und der Text auf dem Screen bestätigt, was wir schon immer ahnten: Bayern gehört nicht zu Deutschland (Text auf dem Screen: „Sie nutzen einen Hotspot außerhalb Deutschlands – es können Roamingkosten entstehen“). Das sorgt natürlich zunächst für einen Lacher – und macht kurz darauf nachdenklich: Roamingkosten? Danke für den Hinweis! Wäre es tatsächlich so, hätte mir die App jetzt Kosten fabriziert, ohne mich zu fragen! Und überhaupt: Warum Roaming-Kosten? Geht es hier nicht um WLAN? Im Prinzip ja, aber die Abrechnung erfolgt ja über die Telekom, und die macht ja Telefon. Folglich: Befindet man sich aus ihrer Sicht im Ausland, fallen Roaming-Kosten an. Kann man verstehen – muss man aber nicht ...

Die nächste Überraschung kommt Stunden später. Wieder zu Hause angekommen, verbindet sich das Gerät nicht mehr mit dem heimischen WLAN. Was ist denn jetzt los? In den Einstellungen nachgeschaut: Dankeschön! Die App hat alle gespeicherten WLANs *deaktiviert*! Man darf sich nun also zunächst wieder überall manuell verbinden. Außer beim nächsten Telekom-Hotspot – außerhalb Deutschlands ...

Müssen wir auf den entsprechenden Komfort nun also verzichten und uns jeweils manuell über die entsprechende Webseite anmelden? Zum Glück gibt es noch Alternativen, die

sogar weitere Anbieter abdecken können, wie beispielsweise abgebildetes **WiFi Web Login**. Auch wenn sich die genannte Webseite wieder einmal ändern sollte, wird diese App dabei nicht unbrauchbar. Man muss sich dann lediglich wieder einmalig manuell anmelden. Denn *WiFi Web Login* schneidet diese manuelle Anmeldung mit (einschließlich etwaiger Eingabefehler) und spielt sie für die automatische Anmeldung wie ein Makro ab. Bei Änderung des Anmeldeformulars muss also lediglich das Makro erneut aufgezeichnet werden, ein Vorgehen, das bei jedem derartigen Netzwerk funktionieren sollte. Davon kann man sich drei Tage kostenlos überzeugen, anschließend muss die App für gut einen Euro käuflich erworben werden, damit sie weiterhin ihren Dienst tut.



WiFi Web Login

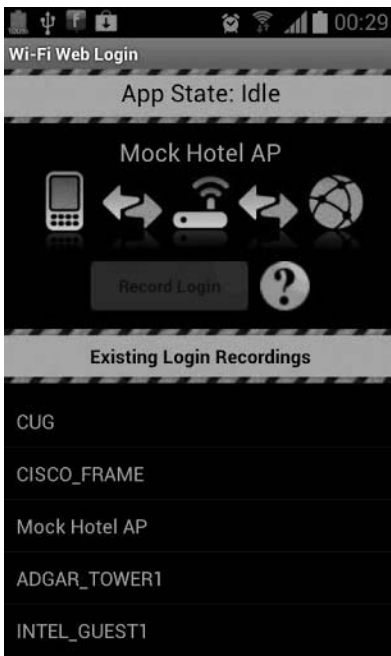


Bild 3.36: *WiFi Web Login* schneidet die Anmeldung einmal mit und spielt sie später als Makro wieder ab

Damit wäre geklärt, wie man sich automatisch anmelden kann. Um dies tun zu können, muss man jedoch zunächst wissen, wo sich ein passendes WLAN befindet – wobei uns wiederum eine ganze Reihe von Apps behilflich sein will, wie etwa das in Bild 3.37 zu sehende *WeFi*, welches ich noch aus „Symbian-Zeiten“ kenne. Die Entwickler sind also bereits seit längerem in diesem Bereich aktiv und verfügen über entsprechende Erfahrungen. Entsprechend groß ist auch die dahinter stehende Community.

Auf der *WeFi*-Website kann man bereits vor Urlaubsantritt nachschauen, wo wohl die besten Hotspots am Ferienort zu finden sind, inklusive Benutzer-Kommentaren natürlich –

das macht eine Community aus. Und vor Ort gibt es dann zusätzlich den „On Demand Scanner“, irgendwie müssen neue Spots ja auch in die Liste kommen. Als Mitglied der Community hat man nämlich die Möglichkeit, neu gefundene Hotspots in die Datenbank einzutragen. Da sich eine recht rege Community an dieser Aktivität beteiligt, wächst die Datenbank beständig. Die Chancen sind also gut, für den Zielort im Voraus eine Reihe passender Hotspots zu finden.

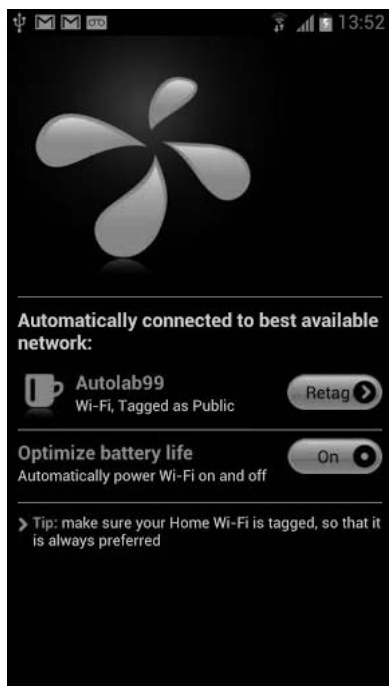
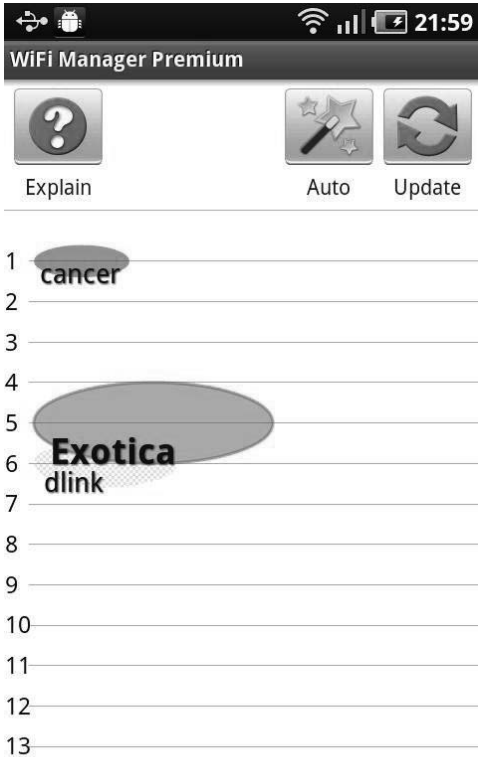


Bild 3.37: *WeFi* hilft beim Finden von Hotspots in der Fremde

Der On-Demand Scanner zeigt übrigens nicht nur an, dass „ein WLAN“ verfügbar ist. Gefundene Netze werden in mehrere Kategorien unterteilt. Das wären zunächst verschlüsselte (also solche, für die man zunächst einen Netzwerk-Schlüssel benötigt) und offene (ohne Verschlüsselung). Doch letztere werden nochmals weiter unterteilt: *WeFi* erkennt automatisch, ob sich hinter einem vermeintlich „offenen Zugang“ noch eine Web-Anmeldung verbirgt. Außerdem werden die Netzwerke besonders hervorgehoben, bei denen eine gute Internet-Verbindung durch die Community bereits bestätigt wurde. Und das sind nur einige der verfügbaren Details.

Einen anderen Weg beschreitet *WiFi Manager*, indem er gefundene Netze grafisch darstellt (Bild 3.38). So lässt sich nicht nur einfach erkennen, welches das stärkste WLAN in Reichweite ist, sondern auch, ob es sich nicht eventuell mit einem anderen überlappt, was die Kanäle betrifft (und die Signalstärke damit wieder relativieren würde). Den einzelnen

Zugangspunkten lässt sich auch eine Beschreibung hinzufügen, so dass man nicht auf den kryptischen Namen allein angewiesen ist. Alles genau beschrieben findet sich auf der Projektseite.



<http://kmansoft.com/sw/>



WiFi Manager

Bild 3.38: WiFi Manager stellt gefundene Netze grafisch dar

Durch In-App Payment über Google Checkout lässt sich ein Premium-Package hinzu erwerben, welches u. a. das Wechseln vorhandener Netze per Widget und das Ausschließen unerwünschter Netze beinhaltet.

Eine ganz spezielle Art zu suchen bietet **SWifis** (Bild 3.39). Die Hauptfunktionalität besteht natürlich auch hier im Auffinden der Netzwerke und dem Verbinden mit selbigen. Aber gerade bei der Suche hat man hier vielfältige Einstellungs-Möglichkeiten: Mindest-Signalstärke? Oder alle Netze mit einer bestimmten Verschlüsselung? Oder einer bestimmten: ESSID bzw. BSSID? Oder nur bestimmte Kanäle? Alles kein Thema mit dieser App, die für ca. einen Euro im Playstore erhältlich ist. Eine Gratis-Testversion ist leider nicht (mehr) verfügbar.



SWifis



Bild 3.39: Mit *SWifis* lassen sich gefundene Netze nach definierten Kriterien filtern

War-Driving

Kriegsspiele? Panzerschlachten, Schiffe-Versenken? Mit all dem hat *War-Driving* herzlich wenig zu tun. Eher mit „da War doch was ...“. Schauen wir also zunächst einmal nach, was genau es mit diesem Begriff auf sich hat, und konsultieren dazu die *Wikipedia*:

Wardriving ist das systematische Suchen nach Wireless Local Area Networks mit Hilfe eines Fahrzeugs. Der Begriff leitet sich von Wardialing ab, einer Methode, durch Durchprobieren vieler Telefonnummern offene Modem-Zugänge zu finden, wobei einige Wardriver die drei Anfangsbuchstaben als Backronym für „Wireless Access Revolution“ sehen (wohl nicht zuletzt, um dem Begriff den martialischen Klang zu nehmen).

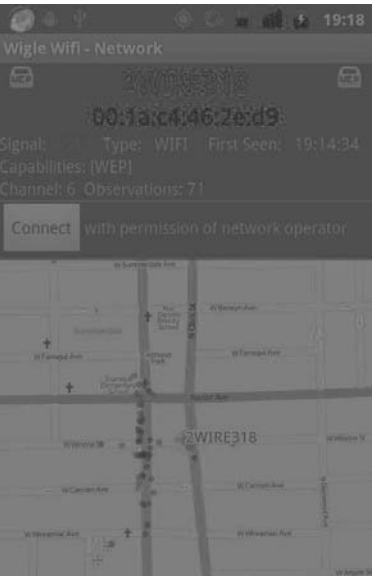


Bild 3.40: Hinter *Wigle Wifi Wardriving* steckt eine Community

Im Prinzip geht es also darum: Wir machen das Gleiche wie auch Google mit seinen tollen Autos, nur in kleinerem Maßstab – und legen eine Karte verfügbarer WLAN-Netze der Umgebung an. Dabei helfen uns Tools wie **Wigle Wifi Wardriving**. Die App lässt sich sehr detailliert konfigurieren und somit auf die eigenen Bedürfnisse anpassen. Gesammelte WLANs können, einen Account vorausgesetzt, zur zugehörigen **Community** hochgeladen werden, wo sie dann allen angemeldeten Mitgliedern (und nur diesen) zur Verfügung stehen. Die eigene Sammlung lässt sich auch gezielt durchsuchen, z. B. mittels **regulären Ausdrücken** über die SSID. Ebenso ist ein Export nach **CSV** und auch **KML** möglich.



Wigle Wifi
Wardriving

Als weiteren Kandidaten möchte ich noch **G-MoN für Android** (Bild 3.41) nennen. Diese deutsche App bezeichnet sich selbst als *WarDriving Scanner & GSM / UMTS Netmonitor und Messtool für Funknetzplaner und Optimierer*. Sie scannt alle in Reichweite befindlichen Netzwerke und speichert deren Daten einschließlich der GPS-Informationen in einer internen SQLite-Datenbank auf dem Androiden ab. Gefundene Zugangspunkte lassen sich per **KML**-Export in *Google Earth* (und sicher auch anderen Anwendungen, welche dieses Format unterstützen) anzeigen, auch ein **CSV**-Export ist möglich.



G-MoN



Bild 3.41: **G-MoN** scannt alle in Reichweite befindlichen Netze – nicht nur WLANs

In Reichweite befindliche WLANs zeigt die App auf Wunsch in einer integrierten Kartenansicht (siehe Screenshot) an. Wie man dort sieht, werden gefundene Mobilfunkzellen

ebenfalls angezeigt; die zu sehende „rote Linie“ weist vermutlich vom eigenen Standort zum ausgewählten (und in der Kopfzeile angezeigten) WLAN.

Weitere und ausführlichere Informationen zu dieser App finden sich im Wiki des Projekts, weitere Apps in der Übersicht im Forum.



<http://www.wardriving-forum.de/wiki/G-MoN>



<http://www.androidpit.de/de/android/forum/thread/429839/>

3.5 Dienste bereitstellen

*Ists möglich, daß so harte Sinnen
Und ungemeine Sprödigkeit
Die zarten Glieder hegen können?
Die mir ein andres prophezeit.
Hier trifft es nicht von Engeln ein,
daß sie dienstbare Geister seyn.*

(Aus: Johann Christian Günther, „Als er sich über ihren Eigensinn beschwerte“)

In diesem Kapitel wollen wir – abschließend zum Thema Netzwerk – einmal betrachten, welche Dienste ein Androide „nach außen“ zur Verfügung stellen kann. Dass ich das Wort „Netzwerk“ hier ein wenig weiter fasse, lässt sich bereits an der Überschrift des ersten Abschnittes feststellen:

Kabelgebunden

Wie jetzt: Kabelgebunden? Der Androide hat doch gar keinen Anschluss für ein Netzkabel! Oder vielleicht doch? Im weitesten Sinne kann man ein USB-Kabel auch als „Netzwerk-Verbindung“ betrachten. Spätestens beim Thema **USB-Tethering** wird da jeder zustimmen. Die einfachste Server-Funktion vergisst man jedoch ganz leicht:

Androide als USB-Stick

Mit dem Aufkommen von USB-Anschlüssen und passenden Speichermedien verlor die Floppy-Disk recht schnell ihren Reiz für den „täglichen Datentransport“. Dank ihrer einfa-

chere Handhabung und der größeren Kapazität überflügelten sie auch zügig die CD und DVD, woran auch die bald erschwinglicher werdenden „Rewritables“ (wiederbeschreibbaren CDs/DVDs) nichts mehr zu ändern vermochten.

Dann kamen die MP3-Player, die nicht viel größer waren als die genannten USB-Sticks, und erfüllten eine Doppelfunktion: Unterwegs konnten sie genutzt werden, um Musik zu hören, den Datentransport übernahmen sie sozusagen nebenbei.

Heute werden beide gleichermaßen durch Smartphones verdrängt: Mir ist kein Smartphone bekannt, für das es keinen MP3-Player und keinen USB-Anschluss gäbe. Und was spricht dagegen, die eingelegte SD-Karte auch als „externe Festplatte“ zu nutzen? Der verfügbare Speicher kann mit dem von USB-Sticks durchaus mithalten, wenn die entsprechende Karte eingelegt ist. Extra Software wird dafür nicht benötigt, und das verwendete Dateisystem ist von Werk aus kompatibel zu allen gängigen Computern.

Eine einfache Sache also – und so mancher greift sich vielleicht jetzt an den Kopf, weil er nicht an diese Möglichkeit gedacht hat. Sein Smartphone hat man ohnehin dabei – warum also noch weitere Dinge einstecken, die man damit bereits abdecken kann? Das Kabel? Auch das ist bei den kurzen Akku-Laufzeiten überall vorhanden. Also hören wir doch auf Altmeister Goethe:

*Willst du immer weiter schweifen?
Sieh, das Gute liegt so nah.
Lerne nur das Glück ergreifen,
Denn das Glück ist immer da.*

(Aus: Johann Wolfgang von Goethe, „Erinnerungen“)

Wem das jedoch nicht „netzwerkig“ genug ist: In einem späteren Abschnitt wird unter *Datei-Server* beschrieben, wie man den „Datenträger“ auch ohne Kabel-Einsatz als solchen vom PC aus nutzen kann.

USB-Tethering

Im Abschnitt *Tethering* habe ich bereits beschrieben, wie man Tethering drahtlos (per WLAN bzw. Bluetooth) bewerkstelligen kann. Welche Gründe könnte es geben, dass man stattdessen lieber ein Kabel nehmen möchte? Da wären tatsächlich ein paar nennenswerte verfügbar:

- Das ans Netz zu bringende Gerät verfügt weder über WLAN noch über Bluetooth, wohl aber über einen USB-Anschluss (selten, aber soll vorkommen).
- Man möchte potenziellen Lauschern ihr „böses Tun“ nicht unnötig erleichtern – in eine drahtgebundene Verbindung können sie sich wohl kaum einklinken.

- Man möchte vermeiden, dass ein zufällig vorbeifahrendes Google-Auto das gerade als Hotspot fungierende Smartphone erfasst und in die Datenbank einträgt.
- Die technischen Voraussetzungen für WLAN-Tethering / Hotspot-Modus sind nicht gegeben (Android < 2.2, kein *root* und keine der verbleibenden Apps funktioniert).



EasyTether

Für den letzten Punkt wurde im genannten Abschnitt bereits *PdaNet* genannt, welches ein Tethering per Bluetooth und USB bewerkstelligen kann. Auch das ebenfalls in der zuständigen Übersicht genannte *EasyTether* kümmert sich um dieses Problem, und zwar bereits ab Android 1.5 (Cupcake). Es wird dafür kein *root* benötigt, und dennoch stehen mit dieser App umfangreiche Features zur Verfügung – wie der Screenshot in Bild 3.42 bereits erahnen lässt. Nicht umsonst ist diese App so gut bewertet (4,3 Sterne bei ca. 18.000 Bewertungen). Einziger

Haken: Die freie Version ist etwas eingeschränkt. Kein HTTPS und auch „Instant Messengers“ werden geblockt. Für die Vollversion werden aber eben einmal knapp acht Euro fällig.

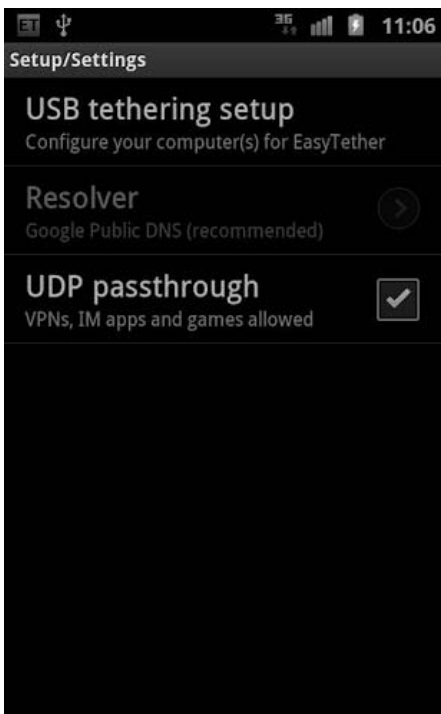


Bild 3.42: *EasyTether* funktioniert ab Android 1.5



Als Alternative wäre noch *Proxoid* zu nennen: Diese App stellt einen Proxy für den Webzugriff von einem über USB-Kabel angeschlossenen Computer bereit, wobei auf letzterem

das Android-SDK installiert sein muss. Anleitungen für die Installation und Konfiguration auf dem PC finden sich im Wiki des Projektes.

Sind es eher die anderen Punkte und läuft auf dem „Hotspot-Gerät“ bereits Gingerbread (Android 2.3), lässt sich USB-Tethering mit Bordmitteln einrichten (siehe Screenshot Bild 3.43): Der entsprechende Konfigurations-Bildschirm findet sich unter *Einstellungen* → *Drahtlos & Netzwerk* → *Tethering & mobiler Hotspot*.



Bild 3.43: Tethering-Einstellungen unter Gingerbread

Kabellos

*Setz die Segel, mach die Leinen los,
da draußen warten deine Träume.
Am Horizont ist Gold, siehst du es scheinen?*

(Aus: Peter Maffay, „Der Mensch auf den du wartest“)

Also dann: Die Leinen Los! Die Kabel weg! Und den Androiden zum Server umfunktio-
nieren. Wozu das gut sein soll? Da fallen mir auf Anhieb viele tolle Dinge ein: Kabelloser
USB-Stick, die Urlaubsfotos ohne Umweg auf einem größeren Bildschirm betrachten ...
Einige davon sollen im Folgenden vorgestellt werden.

Für all diejenigen, die nicht alles separat lesen, aber alles haben wollen, lohnt sicher ein Blick auf die App **Servers Ultimate**. Hier scheint wirklich nahezu alles integriert, was in diesem Bereich möglich ist.



Bild 3.44: Servers Ultimate
bietet ein Komplettpaket verschiedener Servertypen



Servers Ultimate

Datei-Server

Das Thema „USB-Stick“ hatten wir ja bereits behandelt. Das einzige „störende Element“ war das benötigte USB-Kabel. Wollen wir doch einmal sehen, ob es nicht verzichtbar ist! Gleich vorab: Mit Bordmitteln sicher nicht, zumindest habe ich bislang noch nichts entdecken können. Doch wie ich Murphy kenne: Unwahrscheinlich ist es nicht, dass eine neue Android-Version das genau dann anbietet, wenn dieses Buch frisch gedruckt ist.



SwiFTP

Beim Thema „Datenserver“ denkt sicher so mancher zunächst an FTP. Dies ist auf jeden Fall die ressourcenschonendste Art, Dateien zu übertragen. Und so kommt beispielsweise **SwiFTP** als handliches Paket daher: Gerade einmal 80 kB Download sind es. Einmal installiert und gestartet, stellt die App einen kleinen FTP-Server auf dem Androiden zur Verfügung, auf den man dann von allen Geräten, die den Androiden erreichen können, Zugriff hat. Bei den meisten Systemen genügt dafür

bereits ein Webbrowser, in dessen Adresszeile man das eingibt, was einem die App als URL anzeigt. Und schon lassen sich Dateien zumindest herunterladen. Bequemer und definitiv in beide Richtungen geht das natürlich mit einem „richtigen FTP-Client“ wie z. B. **FileZilla** (sowohl unter Windows als auch unter Linux und auf dem Mac).



<http://ppareit.github.com/swiftp/>

Bild 3.45: *SwiFTP* ist ein kompakter, funktionsgeladener FTP-Server

Per Port-Forwarding (oder durch Nutzung eines vom Entwickler bereitgestellten Proxies) lässt sich darüber hinaus auch von beliebigen Orten über das Internet auf diesen Dienst zugreifen. Das gilt bei Nutzung des genannten Proxy sogar, wenn man selbst mit dem Androiden unterwegs und lediglich in das „mobile Netzwerk“ eingebucht ist.

Leider ist diese App aus dem Playstore verschwunden, und der Entwickler hat sie für tot erklärt, da er keine Zeit mehr für die Weiterentwicklung hat. Glück im Unglück: Ein anderer Entwickler hat sich des Projektes angenommen und entwickelt die App weiter! Auf der neuen Projektseite finden sich nicht nur ein paar hilfreiche Informationen; hier kann man auch die .apk-Datei herunterladen.



FTPServer

Bild 3.46: *FTPServer* erlaubt die Einschränkung des Zugriffs auf bestimmte Verzeichnisse (chroot)

Als Alternative wäre noch der **FTPServer** zu nennen. Auch diese App ist „klein und handlich“. Zwar wird hier kein eigener Proxy angeboten, dafür gibt es jedoch andere Funktionen: So lassen sich User „chroot“en (d. h. ihr Zugriff wird auf ein ausgewähltes Verzeichnis inkl. Unterverzeichnisse eingeschränkt), der Server auf einzelne definierte WLANs beschränken u. a. m. Um einem „Abriss“ der WLAN-Verbindung vorzubeugen, kann die App den Standby-Modus deaktivieren.



Samba Filesharing

Wem FTP zu spartanisch ist, der kann z. B. zu *Samba* greifen. Der Name geht auf die Bezeichnung des verwendeten Protokolls zurück: SMB („a“ an passenden Stellen einfügen) steht für Server Message Block, vielen auch einfach als „Windows-Freigaben“ bekannt. Mit diesen „Laufwerken“ kann Windows also von Haus aus (und Linux dank Samba ebenso) prima umgehen, der Androide wird einfach als Laufwerk in das lokale Dateisystem eingebunden, allerdings mit der in Bild 3.47 abgebildeten App **Samba Filesharing** laut ihrer Beschreibung nur das „external Storage“, also die SD-Karte. Was mich persönlich irritiert, denn mit den geforderten root-Rechten sollte auch ein Zugriff auf den internen Speicher sowie dessen Freigabe kein Problem darstellen? Wie dem auch sei: Unser eingangs gesetztes Ziel eines „drahtlosen USB-Sticks“ ließe sich hiermit umsetzen.



Bild 3.47: *Samba FileSharing* bindet den Androiden in das Windows-Netzwerk ein

Eine weitere Möglichkeit der direkten Einbindung in das lokale Dateisystem ist mittels *WebDAV* gegeben. Von Haus aus unterstützen dies sowohl Linux als auch Mac OS, für Windows muss die entsprechende Client-Software separat besorgt werden. Wie die Einrichtung unter allen drei Systemen vonstatten geht, ist auf der Website von *DavDrive* be-

schrieben. Damit ist die Server-App für Android benannt: **DavDrive** (Bild 3.48) stellt die SD-Karte (und in der Vollversion auch den internen Speicher, diesen allerdings nur im Lesezugriff) per WebDAV zur Verfügung. Die Vollversion lässt sich für knapp einen Euro im Play-store erwerben und stellt zusätzlich zur Basis-Funktionalität verschlüsselte Verbindungen (HTTPS), Autostart-Funktionalität, Tasker/Locale Plugin und einiges mehr zur Verfügung.



DavDrive



Bild 3.48: **DavDrive** ermöglicht den Zugriff per WebDAV

Steht die Sicherheit im Vordergrund, muss natürlich auch SSH Erwähnung finden. Mittels dieses Netzwerkprotokolls lassen sich nicht nur Dateien übertragen; die Möglichkeit eines Terminal-Zuganges (also zur Kommandozeile des Servers) ist ebenfalls gegeben.

Einen passenden Server stellt **QuickSSHd** (Bild 3.49) auf dem Androiden zur Verfügung. Die Implementierung dieser App basiert auf Dropbear, was als besonders ressourcenschonend gilt. Auch wenn *root* nicht zwingend vorausgesetzt wird, bringt er in diesem Zusammenhang mindestens einen Vorteil mit: Die Verwendung des Standard-Ports 22 wird dadurch möglich, so dass der entsprechende Parameter beim Zugriff (zur Angabe des zu verwendenden Ports) entfallen kann. Leider bietet der Entwickler keine Gratis-Version zum Test an; aber ein Euro ist nun wirklich keine zu große Ausgabe.



QuickSSHd



Bild 3.49: QuickSSHd bietet verschlüsselten Zugriff über SSH

Zum Abschluss sei mit **File Expert** (Bild 3.50) noch ein ganz spezieller Kandidat genannt. Er ist weit mehr als nur ein Dateiserver. Man muss sogar soweit gehen zu sagen: Das macht er nebenbei. Hauptsächlich will die App ein vollwertiger Datei-Manager sein, mit allem, was dazu gehört: Kopieren, Verschieben, Umbenennen von Dateien und Ordnern, Zugriff auf Daten im Netz per SMB, FTP, SFTP sowie FTPS, Unterstützung für Archive (ZIP/RAR/GZIP/TAR/TGZ/BZ können wie Ordner navigiert und betrachtet werden, ZIP-Dateien lassen sich auch erstellen), Anzeige von Texten und Bildern ... Sogar ein App-Manager ist integriert.



File Expert

Im Umfeld dieser Übersicht sind jedoch die Server-Eigenschaften hervorzuheben. Und hier punktet **File Expert** mit der Bereitstellung eines FTP-, eines Bluetooth- und eines Web-Servers. Über alle drei lässt sich im WLAN drahtlos auf die Daten des Androiden zugreifen. Es können Dateien hoch- oder heruntergeladen, Dateien und Ordner umbenannt oder gelöscht werden – alles über ein einfach gehaltenes Interface.



Bild 3.50: *File Expert* ist weit mehr als nur ein einfacher Datei-Server

Zu den meisten hier genannten Apps gibt es natürlich noch weitere Alternativen. Sie alle in diesem Kapitel zu beschreiben, würde ein wenig zu weit gehen, daher finden sie sich, wie gewohnt, in einer Übersicht im Forum von AndroidPIT.

Web-Server

Die Web-Server möchte ich grob in drei Kategorien einteilen. Die erste befasst sich, wie bereits die im vorigen Abschnitt beschriebenen Server, mit der Bereitstellung von Dateien, dient also in erster Linie dem Dateiaustausch. In der zweiten Kategorie finden sich Web-Server, die vorwiegend Inhalte (statische Webseiten) bereitstellen. Und schließlich soll es auch noch solche geben, die Support für Skriptsprachen wie PHP bieten. Eine Übersicht zu diesen dreien findet sich im Forum.

WiFi File Transfer (Bild 3.51) stellt das lokale Dateisystem ausschließlich per HTTP im WLAN zur Verfügung. Über eine ansprechende Web-Oberfläche lassen sich Dateien hoch- und herunterladen (auch im Batch-Betrieb, also mehrere auf einmal), umbenennen, kopieren, es lassen sich ZIP-Archive erstellen oder auspacken und mehr. Für die



<http://www.androidpit.de/de/android/forum/thread/438399/>



<http://www.androidpit.de/de/android/forum/thread/438200/>



WiFi File Transfer

Betrachtung von Fotos steht sogar eine integrierte Thumbnail-Galerie zur Verfügung. Die Einschränkung der Gratis-Version besteht in einer Limitierung beim Upload: Dateien größer als 4MB werden nicht unterstützt (wohl aber in der Kaufversion – die mit 4,9 Sternen eine absolut spitzenmäßige Playstore-Bewertung vorweisen kann).

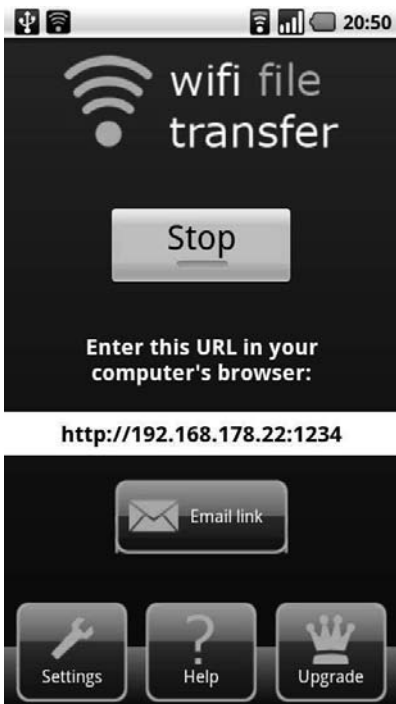


Bild 3.51: *WiFi File Transfer* stellt das lokale Dateisystem per HTTP im WLAN zur Verfügung



Wireless File Transfer

Auch *Wireless File Transfer* (Bild 3.52) erlaubt einen Zugriff auf die im Androiden gespeicherten Dateien über das lokale WLAN. In der Kaufversion sind zusätzlich noch ein lokaler Datei-Manager, ein App-Manager und mehr mit an Bord. Die Web-Ansicht ist in beiden Fällen recht ansprechend und ermöglicht das Anzeigen, Hoch- und Herunterladen, Löschen sowie Umbenennen von Dateien. Darüber hinaus wird auch die Installation von Apps mit einem Klick angepriesen.



Bild 3.52: Auch *Wireless File Transfer* bedient sich des Web-Protokolls HTTP

Mit *kWS* (Bild 3.53) begeben wir uns zu den „Content Servern“, also jenen Web-Servern, die sich um den kompletten Webservice kümmern. Unter Android beschränkt sich dies zumeist auf sogenannten „statischen Content“, also reine HTML-Seiten mit Bildern etc.



Bild 3.53: Mit *kWS* lässt sich eine eigene kleine Homepage hosten



kWS

Die Unterstützung von Skriptsprachen bildet da eher die Ausnahme. *kWS* bietet in dieser Hinsicht zumindest **SSI** für grundlegende Dinge. Dennoch ist die App mit weniger als 100kB Download ein Leichtgewicht und bringt in dem kleinen Paket noch einiges mehr unter: Verzeichnis-Indexe, Resumable File-Downloads, Zugriffsschutz (Basic und Digest Authentication) – sogar Verzeichnis-Downloads (.tar, .tgz und .zip) und ein integrierter DynDNS Updater sind mit dabei. Bis zu zwanzig parallele Verbindungen sind möglich, auch Protokolldateien (Log-Files) werden erstellt.

Noch mehr bietet die Pro-Version, die sich für weniger als zwei Euro im Playstore erwerben lässt: Sie beherrscht außerdem SSL/TLS für gesicherte Verbindungen (HTTPS), komprimierte Übertragung (gzip), Verzeichnis-Indexe in den Formaten JSON und XML und bietet weitere zusätzliche Features.



Bild 3.54: Einen Mini-Web-Server stellt auch **ServDroid.web** zur Verfügung



ServDroid.web

Wer auf SSI verzichten kann, findet in **ServDroid.web** (Bild 3.54) eine Alternative. Diese App nimmt ebenfalls nicht allzu viel Platz weg. In Sachen Funktionsumfang reicht sie an *kWS* vielleicht nicht heran, muss sich aber auch nicht gerade verstecken: Personalisierte „404 Seiten“ („Dokument nicht gefunden“, dito für weitere Fehler), bei eingehendem Request vibrieren, Protokollierung – für die wichtigsten Dinge

und ein paar Extras ist auch hier gesorgt. Dankbare Nutzer haben die Möglichkeit einer Donation in Höhe von einem, zwei oder (zusammengenommen) drei Euro.

Zu guter Letzt noch ein Wort zu einem ganz speziellen Kandidaten, der bereits im Abschnitt 2.7 *Androiden vom PC aus verwalten* vorgestellt wurde: Der *PAW Server* ist ein mächtiges Instrument, das u. a. auch einen Web-Server integriert hat. Und selbiger bringt auch Support für Skriptsprachen mit, was zumindest für Webentwickler interessant sein dürfte. Da wäre zum einen die eigene Skriptsprache, mit der sich auch zahlreiche Systeminformationen darstellen lassen, zum anderen wird über ein Plugin zusätzlich PHP unterstützt.

Medien-Server

Zur Abwechslung einmal kein Verweis auf eine Übersicht, da ich an dieser Stelle nur eine einzige App benenne. **Media Show** stellt die Galerie des Androiden auf einfache Weise für jedes Gerät im lokalen Netz zur Verfügung, welches über einen Web-Browser mit Adobe-Flash-Unterstützung verfügt. Das sollte auf jeden PC und Mac i. d. R. zutreffen – und so braucht sich nicht der gesamte versammelte Freundeskreis um das kleine Display eines Androiden drängeln, um die Bilder von der letzten Party zu begutachten.



Media Show



Bild 3.55: Mit **Media Show** lässt sich die Fotosammlung des Androiden bequem am PC betrachten – und von dort aus verwalten

Und wer hat's erfunden? Die Schweizer. Naja, zumindest sitzt das Team in der Schweiz und doktert nach Feierabend an dieser App. Eine gelungene Arbeit, wie ich finde. Die App wird

natürlich auf dem Androiden installiert und stellt die Quelldaten (Fotos und Videos) per WLAN bereit. Die in den Browser einzugebende Adresse wird nach Start des Service in der App angezeigt. Das notwendige Flash wird aus dem Netz nachgeladen, und schon steht dem Vergnügen nichts mehr im Weg!

Doch das ist noch nicht alles: Die Androiden-Galerie lässt sich so auch am Computer bearbeiten. Man kann Fotos herunterladen, online bearbeiten, via Flickr, Facebook und Twitter mit anderen teilen und mehr.

4 Tuning

4.1 Einleitung und Überblick

Im vierten Teil dieses Buches wenden wir uns schließlich dem Tuning zu: Wie lässt sich möglichst viel aus dem Androiden herausholen?

Zuerst einmal sollte geklärt werden: Möglichst viel wovon? Altbekannt: Wenn ein Manta-Fahrer in den Supermarkt geht, will er Mantarinen und Tunefish. Und später dann die Kiste tiefer legen (ja, auch die auf dem Friedhof). Aber was wollen wir nun mit dem Tunen erreichen?

Prinzipiell gibt es zwei Richtungen: „Schneller, weiter, höher“ (Performance/Geschwindigkeit) und „langes Durchhaltevermögen“ (Akku-Laufzeit); bis auf einige wenige Ausnahmefälle schließen sich diese Tuning-Ziele i. d. R. gegenseitig aus. Des Weiteren gilt es zu beachten: Was kann „Otto Normalanwender“ umsetzen, und was richtet sich eher an „Nerd Root“? Bevor wir uns auf die Details einlassen, zunächst eine Kurzübersicht über die Möglichkeiten:

Generelle Maßnahmen

Toll, dass es Dinge gibt, die beides bedienen: Mehr Speed ohne zusätzliche Akku-Belastung nimmt man gern, längere Akku-Laufzeiten ohne Performance-Einbußen ebenso. Utopisch? Zu wahr, um schön zu sein? Es gibt sie aber wirklich, die derartigen Tuning-Maßnahmen.

Aufräumen:

- nicht mehr verwendete/benötigte Apps deinstallieren
- Cache bereinigen
- selten genutzte Apps am automatischen Starten hindern (ggf. wird root benötigt)
- häufig genutzte Apps möglichst im internen Speicher installieren (auch an die ständig im Hintergrund laufenden Apps denken). Dieser hat einerseits kürzere Zugriffszeiten (ist also schneller) und andererseits weniger Energiebedarf bei Zugriffen.

Live-Wallpaper und sonstige „animierte Dauerrenner“: Wer darauf verzichten kann, sollte es tun, denn die nuckeln anständig am Akku und knabbern auch gern an der CPU!

Auf Task-Killer weitgehend verzichten. Diese tragen i. d. R. weder zu verbesserter Performance noch zu längerer Akku-Laufzeit bei – sondern ganz im Gegenteil.

Ein netter Nebeneffekt der ersten beiden Aufräumaktionen: Es wird wieder interner Speicher frei. Eine Nebenwirkung, die man auch gern mitnimmt.

Bessere Akku-Laufzeit

Warum nur ist am Ende des Akkus noch so viel Tag übrig? Eine Frage, die sich sicher manch einer (und nicht nur einmal) schon gestellt hat. Was hier Abhilfe schafft, geht nicht selten zu Lasten der Performance, aber häufig so unmerklich, dass man es durchaus in Erwägung ziehen kann:

- WLAN komplett abschalten, wenn's nicht gebraucht wird. Das spart enorm (siehe Anhang!) und lässt sich auch automatisieren. Die Verzögerung bei der bedarfsmäßigen Aktivierung ist zu verschmerzen.
- Wer kein mobiles High-Speed benötigt: 3G aus, das frisst auch ganz nett. Wer es hin und wieder benötigt, kann es bei Bedarf aktivieren. YouTube per mobilem Datennetz macht mit 2G aber natürlich weniger Spaß.
- GPS benötigt im Standby zwar so gut wie keinen Saft – aber wenn es deaktiviert ist, kann auch keine „böse App“ für „Werb Standort“ darauf zugreifen.
- Helligkeit des Displays weitmöglichst herunterregeln. „Aufdrehen“ dann im Bedarfsfall. Das Display-Timeout möglichst kurz (aber nicht zu kurz) einstellen.
- Die Datensynchronisierung muss evtl. nicht (für alle Apps) ständig laufen (Hintergrunddaten deaktivieren, Intervalle anpassen, Apps ausnehmen).
- Verschiedene Apps helfen ggf. bei der Laufzeit-Verlängerung, indem sie gewisse Aufgaben automatisch ausführen (*JuiceDefender*, *GreenPower*, *BatterySaver* ...).
- Gute Pflege nimmt der Akku gern an (Temperaturbereich, Ladezustand, Kalibrierung).
- *root* und Modder: CPU nicht über-, sondern ggf. eher untertakten. Ich weiß, das klingt nicht besonders „cool“ – spart aber Akku. Und auch dies lässt sich automatisieren: So benötigt man beispielsweise bei ausgeschaltetem Display und zu nachtschlafender Stunde meist nicht die volle CPU-Last.



Mehr Speed

Speedy Gonzales überholen mit einem Androiden der ersten Generation? Da stehen die Chancen eher schlecht. Aber neben den **generellen Tipps** gibt es auch hier noch die eine oder andere Spezialität:

- RAM bereinigen (Android-interne Einstellungen optimieren). Die persönlich richtige Mischung aus „verfügbarem RAM“ und „schnell verfügbaren Apps“ festlegen.
- Eventuell Swap-Space nutzen (braucht *root*).
- Nur für bestimmte Situationen, in denen es darauf ankommt: CPU ggf. leicht übertakten. Frisst aber auch mehr Akku. Und benötigt *root*.



4.2 Generelle Tuning-Maßnahmen

Nicht mehr verwendete/benötigte Apps deinstallieren

Ein unnötiger Vorschlag? Verstehe: Auch ein Wildfire oder gar ein Gerät mit noch weniger internem Speicher im Einsatz? Trotzdem nicht für jeden selbstverständlich, aber: Alles raus, was keine Miete zahlt!

Und was soll das bringen? Mehrere Dinge. Zuerst einmal das offensichtliche: Es wird wieder interner Speicher frei, der zuvor von der App belegt wurde, aber auch der, den die Daten der App mit Beschlag belegten, und der Platz, den der Cache der App in Anspruch nahm.

Gerade bei Geräten mit wenig internem Speicher kann das einiges bringen, denn dieser frei gewordene Platz steht nicht nur neuen Apps zur Verfügung, sondern kann auch als Cache genutzt werden (das geschieht automatisch). So muss beispielsweise eine noch aktuelle Datei nicht aus dem Netz neu geladen werden, was schnelleren Zugriff und geringeren Stromverbrauch bedeutet.

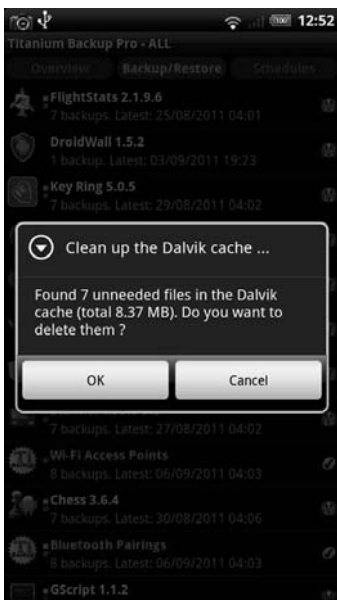


Bild 4.1: Titanium Backup räumt den Dalvik-Cache auf

Hat man eine Reihe von Apps auf diese Weise ins Nirwana befördert, kann man sich als Wurzelmensch (also Android-User mit *root*) auch Gedanken um die Bereinigung des *Dalvik-Cache* machen. Hier sind ja ebenfalls Lücken entstanden, und eine Reorganisati-





on würde für einen schnelleren (und kürzeren, also Akku-schonenderen) Zugriff sorgen. Eine Möglichkeit dazu bietet *Titanium Backup Pro* mit der Option „Cleanup Dalvik Cache“ (Bild 4.1). Alternativ bieten die meisten Custom-Recovery-Menüs eine entsprechende Option, den Dalvik-Cache komplett zu löschen – beim nächsten Boot wird er dann automatisch neu aufgebaut.

Ja toll – und wie wird man eine App nun los? Dazu kann man auf die Bordmittel zurückgreifen, von denen üblicherweise zwei zur Verfügung stehen. Auf jedem Androiden findet sich in den Einstellungen die Möglichkeit, die installierten Anwendungen zu verwalten (üblicherweise unter *Einstellungen* → *Anwendungen* → *Anwendungen verwalten*). Hier wählt man die zu deinstallierende App aus und betätigt den passenden Button – naheliegenderweise ist dieser meist mit *Deinstallieren* beschriftet. Ist er ausgegraut und lässt sich nicht betätigen, muss man evtl. zunächst die App beenden (über den Button *Stoppen erzwingen*). Klappt es danach noch immer nicht, handelt es sich um eine „System-Applikation“ – ohne *root* lässt sich eine solche nicht entfernen.

Das zweite Bordmittel ist die Playstore-App. In dieser sollte sich die zu entfernende App unter *Meine Downloads* wiederfinden und ebenfalls mit einem *Deinstallieren*-Button versehen sein. Ist dies nicht der Fall, wurde die App nicht über den Playstore installiert, und es handelt sich evtl. gar um eine System-App. Da hilft uns die Playstore-App dann nicht weiter.

Als alternative Uninstaller kommen zahlreiche Apps in Betracht. Da wäre zum Beispiel das bereits genannte *AppMonster*, das neben der Sicherung auch eine Deinstallation von Apps ermöglicht. Ebenso kommen spezielle Deinstallations-Apps wie *Fast Uninstaller* oder *Shake-Uninstall* in Frage. Letzteres bietet einen spaßigen Ansatz: Man öffnet die zu entfernende App und schüttelt zum Deinstallieren das Gerät (daher auch der Name). Also einfach immer laufen lassen: Wenn es einen dann bei einer App schüttelt, wird sie automatisch entfernt. Was aber wiederum nur bei selbst installierten Apps klappt. Und Werbung lässt sich so nicht entfernen.



Für die vom Hersteller vorinstallierte sogenannte **Bloatware** kann der Wurzelmensch wieder auf das bewährte *Titanium Backup* zurückgreifen. Um dabei nicht zu viel Schaden anzurichten (indem man beispielsweise eine vom System wirklich benötigte App versehentlich löscht) und sich ebenso wenig die Möglichkeit eines **OTA**-Updates nicht zu verbauen, lassen sich unerwünschte System-Apps damit auch einfach „einfrieren“: Sie werden dann nicht gelöscht, sondern lediglich „kalt gestellt“ – sind also schlicht „unsichtbar“, werden nicht mehr gestartet und stören damit auch niemanden. Eine Möglichkeit, die übrigens auch das kostenlose (und nur ca. 150 kB große) *App Quarantine* anbietet.



App Quarantine

Eine abschließende gute Nachricht: Ab *Ice Cream Sandwich* (Android 4.0) ist die Funktionalität zum „Einfrieren“ von Bloatware zur Nutzung durch den Endanwender von Haus aus ins System integriert.

Cache bereinigen

So ein Cache ist schon etwas Feines. Er sorgt nicht nur für schnellere Zugriffe, sondern spart dabei auch gleich noch CPU, Traffic und Akku. Was also ist daran so schmutzig, dass es bereinigt werden muss?

Dafür ganz kurz die allgemeine Erklärung, wie ein Cache funktioniert. Es handelt sich dabei um eine Art „temporären Zwischenspeicher“, beispielsweise für Dateien, die aus dem Internet geladen werden (wenn lokal vorhanden und aktuell, spart das ein kosten- und zeintensiveres Nachladen) oder um die Ergebnisse einer aufwendigeren Berechnung (spart dann Zeit, CPU und Akku) zwischenzuspeichern. Soweit ist das alles prima und überaus nützlich.

Problematisch wird es erst dann, wenn kein Verfallsdatum festgelegt wurde und keine automatische Bereinigungsaktion stattfindet – dann sammelt sich im Cache nämlich überwiegend „Hausmüll“, den niemand mehr braucht. Der wiederum bremst den Zugriff auf sinnvolle Cache-Daten und belegt wertvollen Speicherplatz, was leider keine Seltenheit ist. Also sprach Zarathustra: Ab und an einmal Hausputz betreiben kann hilfreich sein. Nicht zu oft natürlich, sonst ist der Cache ja insgesamt nutzlos. Wie oft eine Bereinigung sinnvoll ist, lässt sich pauschal schwer sagen – doch spätestens wenn der interne Speicher knapp wird, ist dies sicher eine der ersten zu ergreifenden Maßnahmen. Negative Seiteneffekte stehen nicht zu befürchten: Findet eine App das gewünschte Element nicht im Cache, wird es einfach neu heruntergeladen bzw. generiert, was auch der Grund ist, warum eine Bereinigung manchmal eine zickige App wieder in die Bahn bringt: Kaputte Elemente im Cache können so etwas verursacht haben. Sind die weg, können sie nicht mehr länger für Probleme sorgen.

Wo geht es nun zum Besenschränk? Mit Bordmitteln heißt es: Unter *Einstellungen* → *Anwendungen* → *Anwendungen verwalten* alle Apps einzeln anwählen und schauen, ob und wie viel Cache sie belegen sowie ggf. den passenden Button zum Leeren des entsprechenden Cache betätigen. Es gibt keine Übersicht, die vielleicht gar noch nach belegter Datenmenge sortiert wäre.

Bis vor Kurzem war das auch das Ende der Fahnenstange für den „Normal-Anwender“. Dinge wie „Alle Caches mit einem Klick löschen“ blieben „Nerd Root“ vorbehalten. Aber das hat sich glücklicherweise geändert.

So bietet beispielsweise **Quick App Manager** (Bild 4.2) mehr als nur die Möglichkeit, alle Caches mit einem Klick zu putzen. Hierfür lässt sich sogar ein Scheduler einrichten, der das automatisch im eingestellten Intervall erledigt und sich nebenbei auch um weitere „historische Daten“ (wie den Verlauf des Webbrowsers) kümmert. Wer das nicht ganz so vollautomatisch mag, kann sich auch bei Erreichen eines konfigurierbaren Limits warnen lassen, etwa wenn der Cache mehr als fünf Megabyte belegt, und dann selbst in der sortierten Liste nachschauen



Quick App Manager

und entscheiden, welche App man bereinigen möchte. Nebenbei kann *Quick App Manager* auch Apps mit potentiell risikobehafteten Permissions anzeigen und bringt einen App2SD sowie einen Task-Manager mit. Für diesen Komfort ist allerdings ein knapper Euro fällig – eine gratis Test-Version konnte ich nicht finden.

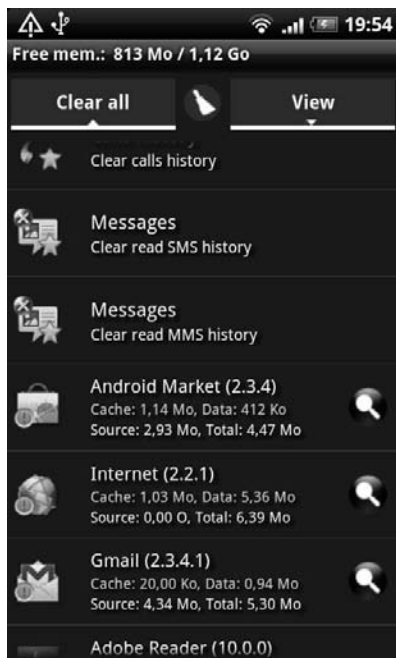


Bild 4.2: *Quick App Manager* bereinigt alle Caches mit nur einem Klick



Quick Cache Cleaner

Wer auf die Extra-Manager sowie den Scheduler verzichten kann, findet in *Quick Cache Cleaner* eine mögliche Alternative. Um Cache und Browserverlauf kümmert sich diese App ebenfalls mit nur einem Klick, auch die Sortierung (nach Name bzw. belegtem Cache) sowie die Einschränkung auf Apps, die überhaupt Cache belegen, beherrscht sie. Und sie ist darüber hinaus auch noch gratis erhältlich.



1Tap Cleaner

Ebenfalls gratis (oder besser: werbefinanziert) gibt es mit *1Tap Cleaner* (Bild 4.3) eine weitere App, die sich sowohl um den Cache als auch um die anderen „historischen Fälle“ kümmert und dabei auch einen Scheduler mit an Bord hat. Nebenbei kümmert sie sich auch um die sogenannten „App Defaults“ und setzt sie bei Bedarf zurück. Das ist hilfreich, wenn man beispielsweise einen alternativen Launcher zum Standard gemacht hat und nicht weiß, wie man diesen Standard nun wieder los wird, um den „alten“ Launcher nutzen zu können (klar geht das auch in dessen Einstellungen unter *Anwendungen verwalten*

– aber warum lange suchen?). Neben diversen Sortiermöglichkeiten lässt sich bei dieser App die Liste der Anwendungen sogar nach Namensbestandteilen filtern. Wer die Gratis-Version ausgiebig getestet hat und den Entwickler belohnen (oder einfach nur die Werbung loswerden) möchte: Mit einem Euro ist man dabei.



Bild 4.3: Auch **1Tap Cleaner** bereinigt die Caches per Knopfdruck

Selten genutzte Apps am automatischen Starten hindern

Ein altbekanntes Lied, nicht nur auf unseren geliebten Androiden: So manche App fühlt sich so furchtbar wichtig, dass sie meint, ständig laufen zu müssen, am besten bereits vor dem Booten. Am schlimmsten sind dabei die Ach-so-tollen Apps, mit denen uns Hersteller und Provider „zwangsbeglücken“ und die „Otto Normalanwender“ nicht einmal beseitigen (sprich: deinstallieren) kann. Kaum ist der Androide gestartet, schon laufen auch Flickr, FM-Radio, Google Maps, Peep ..., ohne dass wir sie darum gebeten hätten. Sie belegen dabei Speicher und verbraten CPU und Akku gleichermaßen.

Da möchte man gern einmal kräftig dazwischenschlagen. Wenn man diese Bösewichte nicht einfach deinstallieren kann (etwa weil es sich um System-Apps handelt und man keine root-Rechte hat oder weil man die betreffende App doch hin und wieder einmal benötigt), kann man diesen Wahnsinn nicht einfach abstellen? Bei mancher App findet sich ein betreffender Punkt in den Einstellungen. Ist dies jedoch nicht der Fall, sieht es ohne *root* recht mau aus.

Ein einfacher Task-Manager ist hier definitiv der falsche Ansatz. Allerdings gibt es einige Apps, mit denen sich das automatische Starten unterbinden lassen soll. Ohne root-Rechte sieht das aber eher so aus, dass die betroffenen Apps nach dem Auto-Start automatisch gekillt werden – und das führt leider häufig dazu, dass so manche App dann einfach wieder neu startet, was in einem Teufelskreis mit Akkufresser und CPU-Heizer enden kann. Es sei denn, man hat sich für **Autorun Manager** (Bild 4.4) entschieden: Diese App kann derartige Kreisläufe erkennen und sieht sodann von einer weiteren Behandlung ab. Als Anwender sollte man dann ebenfalls davon Abstand nehmen, eine Behandlung erzwingen zu wollen.



Autorun Manager

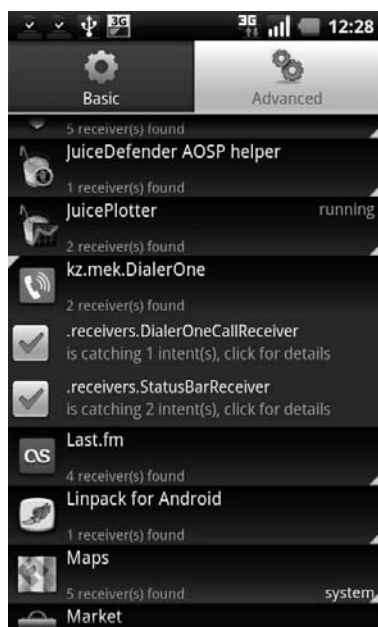


Bild 4.4: Im root-Modus kann **Autorun Manager** alle Startrampen gezielt ansprechen



Weitaus bessere Chancen hat man, wenn man mit root-Rechten ausgestattet ist – und zwar beispielsweise mit gerade genannter App. Diese ist im erweiterten („Advanced“) Modus nämlich in der Lage, automatische App-Starts von vornherein zu unterbinden. Um automatisch gestartet zu werden, muss eine App sich nämlich bei ihrer Installation für die gewünschten Ereignisse (sogenannte „Intents“) registrieren. Nur mit vollen Systemrechten (oder per Deinstallation der App) kann man diese Registrierung wieder auflösen. Genau das geschieht an dieser Stelle, und so hat man volle Kontrolle darüber, wann eine App automatisch starten darf. Nicht nur das „Nach-dem-Booten-Starten“ lässt sich hier abschalten, sondern beispielsweise auch Dinge wie „bei eingehendem Anruf“ oder „nach hergestellter WLAN-Verbindung“, „USB angeschlossen“ ...



Natürlich lassen sich einzelne „Intents“ unabhängig voneinander deaktivieren und diese Aktion später ggf. wieder rückgängig machen, sollte dies notwendig werden. Zu beachten ist jedoch: Vor Deinstallation des *Autorun Manager* sollte man die ursprünglichen Einstellungen wieder herstellen – andernfalls ist dies nur durch Neuinstallation der betroffenen Apps möglich, was sich bei System-Apps als zumindest schwierig darstellen dürfte.

Autorun Manager ist aus meiner Sicht in diesem Bereich die beste Wahl, zumal es auch noch gratis verfügbar ist. Als Alternative käme eventuell noch **Autostarts** (Bild 4.5) in Frage, das nach dem gleichen Prinzip arbeitet (Deaktivieren von Intents), jedoch knapp einen Euro kostet. Auch bei dieser App gilt es, vor der Deinstallation die ursprünglichen Einstellungen wiederherzustellen.



Autostarts



Bild 4.5: Auch **AutoStarts** kann unerwünschte Starts verhindern

Jetzt sollte man aber nicht einfach wild alles abschalten, was einem vor die Flinte (oder besser: unter die Finger) kommt – von System-Apps am besten ganz die Finger lassen (solange man nicht weiß, was man da tut). Sollte eine App sich anschließend irgendwie seltsam verhalten, kann man natürlich alles wieder rückgängig machen (oder die betroffene App einfach neu installieren). Aber warum gleich von vornherein für Probleme sorgen? Wenn man sich auf Dinge beschränkt, die relativ klar und einleuchtend sind, lassen sich Probleme vermeiden. Besonders Ausschau halten sollte man nach folgenden Intents:



- *After Startup* (Nach dem Booten), aka *BOOT_COMPLETED*: Hier soll etwas nach dem Booten (also nach jedem Systemstart) geschehen.
- *Connectivity Changed* (Netzwerkstatus geändert): Darauf lauscht u. a. der Location-Service von *Google Maps*, um die neuen Zellen zur Übertragung an Google im *LocationCache* abzulegen.

Natürlich sollte man sich hier jeweils fragen, ob das nicht eventuell doch sinnvoll sein kann. In der Regel hat man jedoch bereits einen „Dauerbrenner auf dem Kieker“, der ständig läuft und nuckelt – womit sich die Frage meist erübrigt.

Wer sich einfach nur einen Überblick verschaffen möchte, welche App sich für welches Ereignis im System registriert hat, kann ebenfalls das gerade genannte *Autostarts* verwenden: Auch ohne root-Rechte lässt sich diese App installieren, arbeitet dann aber nur im reinen Lese-Modus.

Um auch den „Otto Normalbenutzern“ ohne *root* noch eine Alternative zu nennen: Da wäre **Startup Auditor**, der Apps nach ihrem Auto-Start automatisch wieder abschießt – auf Wunsch auch mehrfach. Um eventuelle „Endlos-Schleifen“ (Start-Kill-Start-Kill-Start ...) muss der Anwender sich bei dieser App jedoch selbst kümmern.



Startup Auditor



Bild 4.6: *Startup Auditor* beendet Apps, die nach dem Booten unerwünscht starten, sofort nach ihrem Autostart wieder

Und bitte nicht wundern, wenn die Nicht-root-Apps scheinbar weniger automatisch startende Apps finden, als *Autostarts* im Lesemodus anzeigt: Das liegt daran, dass erstere nicht alle „Startrampen“ prüfen, sondern sich auf die gängigsten beschränken. Die volle Power bleibt also wieder einmal „Nerd Root“ vorbehalten.

Das Märchen vom Task-Killer

Viele „alte Hasen“ schwören darauf: Task-Killer seien das ultimative Mittel, das System flüssig und den Strombedarf niedrig zu halten. Von genügend anderen Anwendern, die definitiv tiefgreifendes Wissen haben, hört man genau das Gegenteil – teilweise sogar bis zu dem Extrem, dass man Task-Killer gar nicht mehr benötigt, da Android sich selbst darum kümmere.

Da haben wir sie also nun: Zwei Statements, die verschiedener nicht sein könnten – beide von Leuten mit viel Erfahrung. Wem soll nun Glauben geschenkt werden? Da liegt es schon fast auf der Hand, dass die Antwort irgendwo in der Mitte liegen muss, also beide Aussagen einen gewissen Wahrheitsgehalt haben.

Es ist durchaus richtig, dass Android sich selbst um den Speicher kümmert und bei Bedarf nicht mehr benötigte Apps aus selbigem herauswirft. Dafür gibt es den *OOM-Killer*: Wird der Speicher knapp (ist das System also Out-Of-Memory), tritt er in Aktion. Aber nur dann. Läuft hingegen eine App Amok und verwandelt die CPU in eine Warmhalteplatte für den Kaffeebecher, fühlt sich der OOM-Killer davon überhaupt nicht angesprochen, solange besagte Amok-App nicht zeitgleich sämtlichen Speicher auffrisst. Dies wäre also ein Fall für den „klassischen Task-Killer“.

Die Frage ist also weniger, *ob* als vielmehr *wann* man einen Task-Killer einsetzen sollte:

- Falsch: „Ich will den Speicher freiräumen“. Dafür ist der „OOM-Killer“ zuständig (siehe Abschnitt *RAM bereinigen* weiter vorne).
- Falsch: „Ich will Akku sparen“. Das geht mit einem Task-Killer i. d. R. eher nach hinten los.
- Richtig: „Eine App hat sich aufgehängt und blockiert [irgendwas]“. Hier ist der Task-Killer angesagt, denn bis der „OOM-Killer“ hier zuschlagen würde ... Und ein Reboot ist nicht gerade die wünschenswerte Alternative.
- Richtig: „Eine App läuft Amok“ (Panik-Mode: Man erwischt gerade eine App dabei, wie sie alle persönlichen Daten inkl. Bankverbindung, Kontostand und Kreditkartennummer auf eine berüchtigte Website hochlädt ...). Oh ja: Abschießen! Oder gleich abschalten.
- Notfalls richtig: Kurz nach Betätigung des Start-Knopfes einer App (wann sonst?) fällt einem auf: Das würde jetzt zu lange laufen, weil [xxx]. Richtigerweise hätte man dann besser gar nicht erst den Knopf gedrückt. Lässt sich die App nicht anders vom „Weitermachen, bis der Arzt kommt“ abbringen und belegt dabei wertvolle Ressourcen (CPU, Netztraffic), ist das „Abschießen“ mittels Task-Manager auch hier die einzige Alternative zum Reboot.

Die generelle Aussage, dass Task-Manager ein tolles Mittel zum Akku-Sparen seien, fängt jedoch definitiv mit „Es war einmal ...“ an. Für Android-Versionen, die vor dem Punkt nur

eine „1“ stehen haben, traf das vielleicht tatsächlich zu. Aktuell ist es jedoch wesentlich häufiger der Fall, dass eine frisch gekillte App binnen weniger Sekunden schon wieder aktiv ist – was bei „automatischen Task-Killern“ zu einem ewigen Kreislauf aus „Start-Kill-Start“ führen würde und alles andere als ressourcensparend ist.

4.3 Längere Akkulaufzeiten erreichen

Kürzlich absolvierte ein Bekannter einen zweiwöchigen Auslandsurlaub. Da er dort eine lokale SIM-Karte einsetzen wollte, um Roamingkosten zu vermeiden, benötigte er ein Reserve-Handy, um auch unter seiner heimischen Rufnummer erreichbar zu sein. Zu diesem Zweck wurde ein „Billig-Telefon“ der Marke Nokia hergenommen und aufgeladen. Das Ladegerät hätte er ruhig zu Hause liegen lassen können: Obwohl nur im Flugzeug abgeschaltet und ansonsten permanent in Bereitschaft, hielt es mit der einen Akkuladung die vollen zwei Wochen durch, einschließlich einiger kürzerer Telefonate.

Zwei Wochen mit einer Akku-Ladung! So manch einer wäre schon froh, wenn er es auf zwei Tage bringen würde! Sind unsere Akkus schlechter geworden, oder woran liegt es?

Wohl eher daran, dass moderne Smartphones mittlerweile vollwertige Computer im Hosentaschen-Format sind. Was musste denn das oben genannte Nokia „leisten“? Kurz gesagt: „GSM-Standby“ und ein paar GSM-Gesprächsminuten. Mehr nicht. Unsere Smartphones sind hingegen permanent online, surfen am liebsten mit 3G und spielen parallel dazu YouTube-Videos ab. Wer nun einen kurzen Blick in die passende Übersicht im Anhang *Leistungsaufnahme verschiedener Komponenten* wirft, sieht den Unterschied deutlich: Würden wir unsere Androiden auch auf Standby reduzieren und sämtliche „überflüssigen“ Dienste deaktivieren, sollten wir eigentlich ebenfalls die Wochenfrist überschreiten können.

In „voller Ausbaustufe“ ist das sicherlich wenig sinnvoll – man hat sich ein Smartphone ja unter anderem wegen all dieser „Extras“ gekauft. Aber gibt es vielleicht Kompromisse? Schließlich fährt ja auch keiner seinen Porsche im fünften Gang mit 220 km/h in die Garage, nur weil er ihn für „schnelles Fahren“ gekauft hat. Ebenso wenig telefoniert man non-stop und schaut auch nicht 24 Stunden pro Tag YouTube-Videos über die 3G-Verbindung.



DrainGuard

Ob da gerade etwas unverhältnismäßig viel Strom zieht, während der Androide beispielsweise eigentlich „ungenutzt“ in der Tasche steckt, verrät die App **DrainGuard** (Bild 4.7). Sie teilt dem Anwender zwar nicht mit, wer der Schuldige ist, doch zumindest warnt sie bereits, wenn der Akku-Sauger am Werk ist, und nicht erst, wenn der Akku bereits leer gesaugt worden ist. Die notwendigen Werkzeuge zum Aufspüren des Übeltäters finden sich im Abschnitt 2.3 unter *System-Info*.

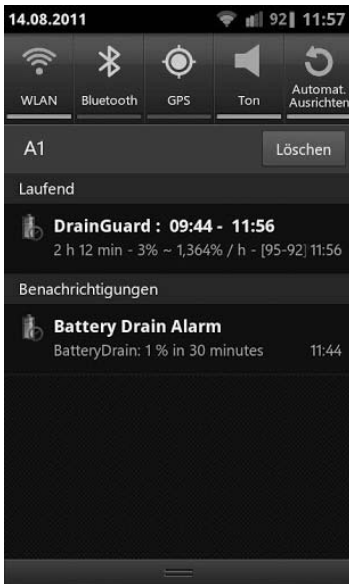


Bild 4.7: *Drainguard* schlägt bei plötzlich hohem Akkuverbrauch Alarm

Deaktivierung ungenutzter Dienste

Wie unschwer in der im Anhang befindlichen Übersicht *Leistungsaufnahme verschiedener Komponenten* erkennbar, gehören die Daten-Dienste (nach der Video-Wiedergabe) zu den größten Verbrauchern. An dieser Stelle ließe sich also am besten sparen – sofern man auf etwas verzichten kann. Was das sein könnte, ist wiederum von Anwender zu Anwender verschieden: Als erstes gilt es daher, das eigene Nutzungsverhalten zu analysieren.

Wer über kein einziges Bluetooth-Gerät verfügt, kann Bluetooth komplett deaktivieren. Im Standby macht das zwar (nach GPS Standby) am wenigsten aus, aber auch Kleinvieh macht Mist. Das passende Häkchen findet sich in den System-Einstellungen unter *Drahtlos & Netzwerke*.

Auf der gleichen Seite findet sich mit *Mobilfunknetze* ein Untermenü, das ein Häkchen für *Nur 2G Netzwerke* anbietet und somit 3G komplett abschaltet. Das bietet ein weit größeres Einsparpotenzial, wenn man auf die schnellere Datenübertragung zum größten Teil verzichten kann; für die „kleinen Dinge“ wie Mail und die Synchronisation der meisten Apps (insbesondere Kalender und Adressbuch) ist 2G definitiv ausreichend. Weniger interessant ist diese Möglichkeit hingegen für diejenigen, die viel mit dem Webbrowser oder der YouTube-App unterwegs sind, ohne dabei auf WLAN-Netze zurückgreifen zu können, da ein Umschalten über dieses Unter-Unter-Menü auf Dauer doch ein wenig umständlich ist. Und spätestens seit Android 2.3 (Gingerbread) ist ein direktes Umschalten per Widget ohne *root* leider auch nicht mehr möglich.

Ähnliches gilt für GPS, das aber glücklicherweise im Standby so gut wie gar keinen Strom verbraucht. Sobald allerdings eine App zur Standortbestimmung darauf zugreift (erkennbar am GPS-Symbol in der Statusleiste – siehe Beispiel-Symbole in Bild 4.8), macht sich auch das deutlich bemerkbar. Wird GPS vom Anwender selbst nur selten genutzt (sagen wir, maximal an einem Tag im Monat oder nur im Urlaub), schaltet man es ebenfalls besser komplett aus – spätestens, wenn man eine dieser werbefinanzierten Apps beim Zugriff erwischt. Das passende Häkchen findet sich im Menü *Standort & Sicherheit*.



Bild 4.8: GPS-Status-Symbole

Bleibt noch unser bester Freund: das WLAN. Wer es gar nicht braucht, der gehört mit Sicherheit einer Minderheit an. Glücklicherweise kann man diesen Dienst mit diversen Schnellumschaltern (vgl. Abschnitt 2.3) nach Belieben schnellumschalten; bei einigen Geräten (und Custom-ROMs) ist der passende „Knopf“ überdies bereits in der Notification-Area integriert.

Ist zwar nicht direkt ein Dienst, passt aber in diese Reihe: Auch die Kamera ist ein besonderer Schluckspecht. Die Kamera-App sollte man daher besser nicht nach Benutzung im Hintergrund weiterlaufen lassen, sondern beenden. Das gilt auch für diverse Barcode-Scanner, die ja auch die Kamera benutzen. Sollte sich ein solcher nicht richtig beenden lassen (was man meist am kontinuierlich starken Akku-Verbrauch erkennen kann), ist wohl ausnahmsweise einmal der Einsatz eines Task-Killers gerechtfertigt.

Display-Einstellungen

Diese bieten sich ebenfalls für potenziell deutliche Einsparungen an: Ein voll aufgedrehtes Display verbraucht wesentlich mehr Strom als ein 2G-Telefonat, während es auf niedrigster Stufe nur gut halb soviel benötigt wie besagtes Gespräch. Hier empfiehlt es sich daher, einen guten Kompromiss zu finden – zum einen die Helligkeit und zum anderen das Timeout (nach welchem Zeitraum der Benutzer-Inaktivität das Display abgeschaltet werden soll) betreffend.

Beides lässt sich mit Bordmitteln im Menü *Display* konfigurieren. Bequemer geht auch das über diverse Schnellumschalter – besonders wenn bei direkter Sonneneinstrahlung ohnehin kaum noch etwas auf dem Bildschirm zu erkennen ist. Die *Automatische Helligkeit* ist leider meist ein wenig zu hell (und damit stromhungrig); die „beste Einstellung“ ist jedoch sehr subjektiv und muss daher individuell ermittelt werden.

Hintergrunddaten und Synchronisierung

Dieses Thema wurde ja bereits unter *Datensynchronisation im Hintergrund* im Abschnitt 3.1 angesprochen: So manche App möchte gern ständig Daten austauschen. Nicht immer ist dies aber nötig: Die wenigsten aktualisieren etwa ihre Kontaktliste mehrmals stündlich, sei es am Androiden oder am heimischen Bürorechner. Was nicht oder nicht ständig aktualisiert werden muss, kann man daher einfach im Menü *Konten & Synchronisierung* abschalten. Ein manueller Abgleich aus der betreffenden App heraus ist in der Regel immer noch möglich.

Nicht jede App trägt sich jedoch an dieser Stelle ein. Bei den meisten lässt sich aber zumindest das Intervall konfigurieren (andernfalls ist es vielleicht ratsam, sich nach einer Alternative umzusehen, bei der dies der Fall ist). Für RSS-Reader reicht in den überwiegenden Fällen ein Intervall von einer Stunde oder höher (zum Einsparen des Datenvolumens kann man das darüber hinaus auch noch auf bestehende WLAN-Verbindungen einschränken).

In Sachen Mail empfiehlt sich, sofern möglich, die Verwendung von *IMAP Push* gegenüber einem ständigen „Pull“: Dabei fragt nicht der Client ständig nach „Gibt es neue Mails?“ (das wäre „Pull“ oder neudeutsch „Pollen“), sondern der Server sagt im Falle des Falles von sich aus Bescheid. Die Information kommt daher im Regelfall sogar früher. Auf den Energieverbrauch bezogen, gilt diese Empfehlung allerdings nur bedingt, da auch bei *IMAP Push* die Verbindung ab und an einen „Refresh“ benötigt. Grob gesagt: Wer bei Eingang einer Mail sofort reagieren muss, ist damit gut dran. Genügt jedoch eine halbstündliche Aktualisierung, ist das altgewohnte „Pollen“ sparsamer.

Viele Apps berücksichtigen auch eine System-Variable, die kundtut, ob eine Datensynchronisation im Hintergrund zur Zeit erwünscht ist. Die Android-API ist hier leider schwammig: Statt die Berücksichtigung verbindlich zu machen („must“), heißt es dort nur „sollte berücksichtigt werden“ („should“). Markanterweise gehören zu den Missachtern an erster Stelle Apps wie *GMail* und *Latitude* – Google geht also wieder einmal mit „gutem Beispiel“ voran. Andere wie beispielsweise *WhatsApp* folgen diesem.



Bild 4.9: Dazzle: Ein Schnellumschalter

Für Apps, die diese System-Variable berücksichtigen, greifen dann wieder die kleinen Schnellumschalter, wie das in Bild 4.9 gezeigte *Dazzle*: In der Abbildung wäre es der zweite Button von rechts, über den mit einmal Antippen die Synchronisation unterbunden (und natürlich zu einem beliebigen späteren Zeitpunkt wieder erlaubt) werden kann.

Verschiedenes

Dann wären da noch verschiedene Dinge, die so selbstverständlich sind, dass man gar nicht daran denkt. Etwa, dass man energiehungrige Apps nicht unbedingt im „Hintergrund“ weiterlaufen lässt, sondern sie beendet. Denken wir beispielsweise an eine Navigations-App: Diese aktualisiert i. d. R. auch im Hintergrund permanent den Standort – bei Verwendung von GPS nicht gerade eine Akku-schonende Tätigkeit. Auch so mancher Barcode-Scanner hält im Hintergrund die Kamera auf Trab. Wieder andere Apps pflegen im Hintergrund fleißigen Netzwerkverkehr, und so manche „Gratis-App“ lädt auch alle paar Sekunden ein neues Werbebanner, selbst wenn es niemand zu Gesicht bekommt. Ergo: Apps, die man nicht mit voller Absicht im Hintergrund behalten möchte (etwa, weil man sie gleich wieder zu verwenden gedenkt) nicht über die „Home-Taste“ sondern – wenn verfügbar – direkt über die „Beenden“-Funktion (häufig über die Menü-Taste erreichbar) oder zumindest über die „Zurück“-Taste verlassen. Bei hartnäckigen Verweigerern, die sich als Stromfresser herausstellen, ist dann ausnahmsweise einmal der Einsatz eines Task-Killers gerechtfertigt.



<http://www.androidpit.de/de/android/forum/thread/409715/App-Reviews-nach-Einsatzzweck>

Bei Apps, die permanent im Hintergrund laufen wollen (und sich partout nicht beenden lassen), obwohl der Anwender das nicht benötigt, sollte man sich nach Alternativen umsehen. Nicht ersetzbare Apps sind selten, häufig gibt es mehrere Apps, die das Gleiche können. Guter Startpunkt für eine Suche ist die zur App gehörige Seite bei AndroidPIT: Dort sind in der Regel handverlesene Alternativen direkt unterhalb der Appbeschreibung genannt. Auch die große Sammlung der App-Übersichten nach Einsatzzweck kann sich als hilfreich erweisen. Ebenfalls einen Blick wert ist in diesem Zusammenhang die App **Mapsaurus** (Bild 4.10) oder auch die dazugehörige Website <http://mapsaurus.com>: App angeben, und schon tauchen passende

Alternativen (mit zugehörigem Playstore-Link) auf. Wählt man diese nun an, geht das Spielchen weiter. Da sollte sich doch etwas finden lassen! Sehr begrüßenswert wäre es allerdings, wenn sich der zuständige Entwickler auf Anfrage des Problems annimmt – und eine Lösung liefert.

Nicht zu vergessen: Widgets. Hinter nahezu jedem Widget verbirgt sich ein zugehöriger Hintergrund-Prozess, der es mit Daten versorgt. Woher soll es sonst über das aktuelle Wetter, die Anzahl laufender Apps, die Speicher-Belegung und all diese Dinge Bescheid wissen? Der Einsatz von sich automatisch aktualisierenden Widgets sollte daher sparsam und mit Bedacht erfolgen. Was man nicht benötigt: runter vom Desktop. Die eventuell zugehörige App steht weiterhin aus dem App-Drawer heraus unabhängig zur Verfügung. Und bei Bedarf lässt sich das Widget jederzeit wieder hinzufügen.



Mapsaurus

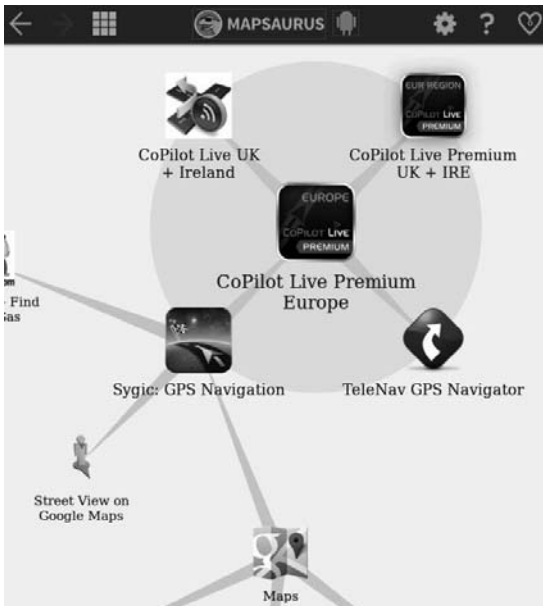


Bild 4.10: Mapsaurus hilft beim Finden alternativer Apps

Einen hab ich noch: So toll und cool sie auch sein mögen, Live-Wallpaper sind besondere Energiefresser. Sie verbrauchen permanent CPU, meist auch noch weitere Ressourcen, und somit anständig Strom. Also besser darauf verzichten, solange einem die Akku-Laufzeit nicht egal ist.

Wer jetzt das „große Fragezeichen“ im Gesicht hat, wie denn „Bösewichter“ wohl auffindig zu machen seien: Ein Blick in Abschnitt 2.3 unter *Monitoring* oder auch *Ausführlichere System-Infos* hilft weiter.

Akku-Pflege

Akkus mögen es, wenn man sie gut behandelt. So kann die Beherrschung einiger kleiner Tipps nicht nur zu einer besseren Laufzeit im aktuellen Ladezyklus, sondern auch zu einer höheren Lebensdauer des kleinen Kraftwerks beitragen. Nichts Kompliziertes, auch spezielles Zubehör braucht es nicht. Vielmehr geht es um das „Gewusst-Was“ und „Gewusst-Wie“. Da ist für jeden etwas dabei.

Zusätzliche Informationen (auch zum Umgang) lassen sich der Wikipedia entnehmen: sowohl für LiIo-Akkus als auch für LiPo-Akkus. Eine kurzgefasste Aufstellung der wichtigsten Fakten findet sich auch bei *sinnvoll-online.de*.



sinnvoll-online.
de/seiten/mobil-
funk/tipps-zur-
akkupflege.php

Temperatur

Aktuelle Androiden verwenden sogenannte Lithium-Ionen-Akkus (LiIo). Für diese Geräte gilt das Folgende: Sie mögen es nicht so warm. Also nicht in die Sonne legen, auch die Hosentasche ist nicht der ideale Aufbewahrungsort. Bevor jemand fragt: Nein, der Kühlschrank auch nicht. Lieblings-Temperatur von LiIo-Akkus: ca. 20°C. Unterhalb von 10°C lässt die Leistungsfähigkeit nach, der „Arbeitsbereich“ wird meist mit 0 bis 40°C angegeben. Einige Androiden setzen auch auf die Weiterentwicklung Lithium-Polymer (LiPo), wie Motorolas *Droid Razr* oder auch *CLIQ*; ebenso eine ganze Reihe Tablets: *Acer Iconia*, *Asus Transformer*, *Samsung Galaxy Tab* u. a. m. Platt gesagt, sind LiPo-Akkus kompakter, dafür aber auch empfindlicher, was den Temperatur-Bereich betrifft.

Laden / Entladen

Eine vollständige Entladung bis zur Selbstabschaltung des Gerätes sollte zwar hin und wieder zur Kalibrierung stattfinden – aber nicht zu häufig: Sowohl LiIo- als auch LiPo-Akkus mögen eine vollständige Entladung nicht so gern. Idealerweise schließt man sie also wieder an das Ladekabel an, bevor der Ladezustand die 50%-Marke unterschreitet. Höhlen-Taucher wissen, wovon ich rede, wenn ich an dieser Stelle den Begriff „Reserve“ in den Raum stelle: Natürlich kann man auch die „unteren 50%“ nutzen – gesünder (in diesem Fall für den Akku) ist es jedoch, darauf nicht angewiesen zu sein. Einen Memory-Effekt kennen weder LiIo noch LiPo, diesbezüglich ist daher nichts zu befürchten.

Den Akku kalibrieren

Der Ausdruck ist ziemlich irreführend. Genau genommen wird nicht etwa der Akku, sondern der Androide kalibriert. Letzterer lernt dabei nämlich, wie es um die tatsächliche Akku-Kapazität bestellt ist und kann seine Statistiken entsprechend anpassen. Damit wird vermieden, dass das Gerät „plötzlich und unerwartet“ bei einem angeblichen Akku-Stand von über 30% „das Zeitliche segnet“ oder aber die Anzeige schnell von 100% auf 1% fällt, um dann noch ein paar Stunden dort stehen zu bleiben – bevor der Akku wirklich leer ist.

Dies geschieht durch einen sogenannten „vollständigen Ladezyklus“. Bildlich gesprochen, wird der Akku dabei einmal von 100% auf 0% und wieder auf 100% gebracht – wobei während des gesamten Zyklus das Ladegerät exakt ein Mal mit dem Gerät verbunden wird (oder auch umgekehrt; auf jeden Fall eine volle Ladung ohne Unterbrechung).

Optimalerweise werden zu Beginn dieses Zyklus noch die Akku-Statistiken gelöscht, was in der Regel jedoch root-Rechte voraussetzt. Doch dieser Schritt scheint eher einem Mythos gezollt, wie Android-Entwicklerin Diane Hackborn laut *XDA-Developers* erklärt: In der `batterystats.bin`-Datei werden laut ihrer Aussage keine Daten der Batterie, sondern ausschließlich die (auch unter *Einstellungen* → *Akku-Verbrauch* einsehbaren) Verbrauchs-



<http://www.xda-developers.com/android/google-engineer-debunks-myth-wiping-battery-stats-does-not-improve-battery-life/>





daten gespeichert. Somit erübrigt sich eigentlich auch der Einsatz der folgenden Apps, mit deren Vorstellung ich dem Mythos dennoch meine Referenz erweisen möchte:

Hilfreich bei der Kalibrierung sind Tools wie das in Bild 4.11 gezeigte **Battery Calibration**. Diese App führt den Anwender Schritt für Schritt durch den Prozess, und übernimmt nebenbei auch die Löschung der gespeicherten Akku-Statistiken aus dem Android-System.



Battery Calibration



Bild 4.11: *Battery Calibration* will bei der Kalibrierung des Akkus helfen

Das Vorgehen ist total einfach: Man startet die App und steckt das Ladekabel an. Anschließend stellt man sicher, dass beide Buttons jeweils ein „grünes Lämpchen“ enthalten, womit die App angewiesen wird, bei Erreichen einer vollständigen Aufladung (100%) den Anwender mit Piepsen zu benachrichtigen, dass es weitergehen kann. Sobald dieser Zeitpunkt erreicht ist, betätigt man den großen Button in der Mitte (das löscht die `battery-stats.bin` aus dem System) und startet den Androiden neu (womit die genannte Datei neu angelegt wird). Ladekabel raus und einmal komplett leerlaufen lassen (mindestens bis 20%, besser weniger); anschließend Ladekabel wieder anschließen und in einem Rutsch wieder vollständig aufladen. Fertig.

Wichtig ist, wie beschrieben, ein vollständiger Zyklus – man könnte es also auch umgekehrt machen. So tut das etwa **Battery Calibrator** (Bild 4.12) und startet am „Nullpunkt des Seins“. 20% Ladung oder weniger, gerade genug, um die `batterystats.bin`-Datei noch vor dem Durchstarten löschen zu können, werden als Anfang des Prozesses gewertet. Das Vorgehen ist ansonsten identisch: Die Datei wird gelöscht, das System neu gestartet und in einem Zug einmal auf 100% und zurück gebracht.



Battery Calibrator

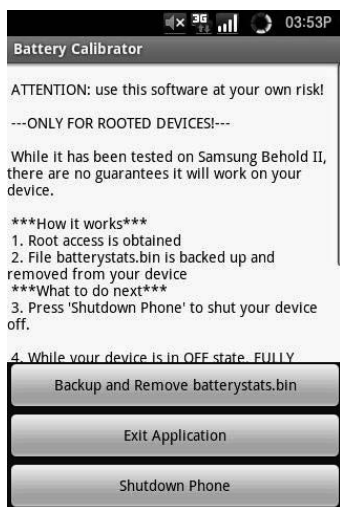


Bild 4.12: Ein weiterer Kalibrier-Helfer ist **Battery Calibrator**

Wo man beginnt, bleibt dem Anwender überlassen – das Ergebnis sollte in beiden Fällen identisch sein: eine korrekte Ladestands-Anzeige. Für das Löschen der Statistik-Datei benötigt es i. d. R. *root*, die genannten Apps vereinfachen lediglich den Prozess.

CPU untertakten

Untertakten? Wollen nicht alle in die andere Richtung? Klar, das kann im Winter ganz praktisch sein: Zusätzlich 3G an, heftig Downloaden, HD-Videos schauen und das Ladekabel dabei angeschlossen – diese Kombination ergibt einen wunderbaren Fingerwärmer, der aber schnell erkaltet, sobald das Ladekabel abgezogen wird – weil der Akku das nicht lange mitmacht.

Wollten wir nicht den Akku zu möglichst langer Laufzeit animieren? Ein geringerer Prozessor-Takt kann dazu beitragen. Nicht umsonst wird in den Medien bereits über eine Fünf-Kern-CPU für Smartphones theoretisiert: Vier Kerne mit ordentlich Power und der fünfte mit geringerer Taktrate sowie weniger Power für die Hintergrundaktivitäten bei abgeschaltetem Bildschirm. Das bekommen wir softwareseitig sicher nicht so ganz hin, können uns dem aber zumindest annähern – *root* vorausgesetzt.



SetCPU

Beispielsweise unter Zuhilfenahme von **SetCPU** und entsprechenden Profilen: Wann immer die volle Leistung nicht benötigt wird, kann die CPU gedrosselt werden, etwa generell bei abgeschaltetem Display oder während unserer Nachtruhe. Empfehlenswert ebenfalls, sofern ein bestimmter Ladestand des Akkus unterschritten wird (damit man es noch zur nächsten Ladestation schafft, ohne dass das Gerät abschaltet).

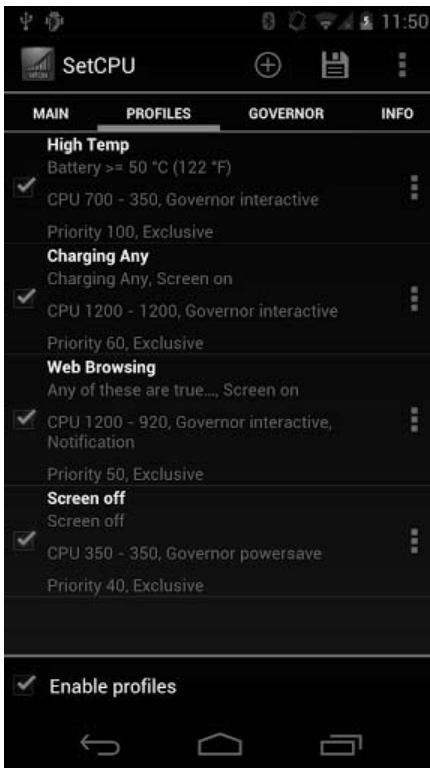


Bild 4.13: Mit *SetCPU* lässt sich die CPU-Taktung verwalten

Eine Steuerung der CPU ist allerdings auch in diverse andere „Automaten-Apps“ integriert. Natürlich in *Tasker* – aber auch in einige der kleinen Helferlein, die im Folgenden kurz vorgestellt werden.

Kleine Helferlein

Menehune? Heinzelmännchen? Eine gewisse Ähnlichkeit lässt sich nicht leugnen: Die Apps, um die es hier geht, bekommt man während ihrer Arbeit nicht zu Gesicht. Sie arbeiten flink und können wahre Meisterwerke vollbringen (wie beispielsweise ein Smartphone mit einer einzigen Akkuladung über mehrere Tage am Laufen zu halten). Der Unterschied: Unsere Helferlein sind auch heute noch am Werkeln und ihre Erfolge lassen sich überprüfen und belegen. Außerdem haben sie im Forum von AndroidPIT eine eigene Übersicht.

Apps für den „Handbetrieb“ wurden ja bereits bei den *Schnellumschaltern* (Abschnitt 2.3) vorgestellt. Zeitschaltuhren, orts- und eventba-



<http://www.android-pit.de/de/android/forum/thread/440187/Uebersicht-Akku-Sparer>



JuiceDefender



<http://www.juicedefender.com/compare/>

sierte Schalter etc. gab es im Abschnitt 2.5 unter *Automatisierung*. Bleibt denn da überhaupt noch etwas übrig? Aber klar doch: Die App-Automaten, die sich speziell dem Energiespar-Thema gewidmet haben: Save Battery!

Der „SaftVerteidiger“ ist die erste App, die man in Foren zu diesem Thema genannt bekommt. Und sie ist sicher auch die umfangreichste und flexibelste App – zumindest in der Ultimate-Version. **JuiceDefender** (Bild 4.14: in der Notification-Area) kommt nämlich in drei Ausbaustufen daher: einer kostenlosen, einer gehobenen (Plus) und einer Deluxe (Ultimate). Und natürlich unterscheiden sich die drei Versionen in ihrem Funktionsumfang, wie eine Übersicht auf der Homepage zeigt.

Alle drei Versionen bieten Widgets (siehe Bild 4.15) sowie Notifications (Bild 4.14) und bieten darüber hinaus mindestens zwei Profile an (normal / aggressiv; extreme / customized kommen ab der Plus-Version dazu). Alle Versionen erlauben die Kontrolle der mobilen Daten (ab der Plus-Version auch WLAN und mit Ultimate zusätzlich Network Switching, AutoSync und Bluetooth). Die Hintergrund-Daten-Synchronisierung lässt sich mit allen drei Versionen steuern (spezielle nächtliche Schedules gibt es dann ab der Plus-Version und mit Ultimate zusätzlich



Bild 4.14: *Juice Defender* verteidigt den „Saft“



Bild 4.15: Zahlreiche Widgets hat *JuiceDefender* bereits mit im Gepäck

Schedules für Peak-Hours und Wochenende). Dinge wie Display-Timeout und -Helligkeit sowie GPS-Kontrolle gibt es nur in der Ultimate-Version, mit Ultimate und *root* lässt sich sogar die CPU steuern. Eine Sonderbehandlung einzelner Apps ist ab der Plus-Version verfügbar.

Das war jetzt ein Stapel Details. Abschließend noch einige Worte zur allgemeinen Funktionalität: Je nach Bedarf regelt *JuiceDefender* die entsprechenden Verbraucher. So lässt sich beispielsweise die Netzwerkverbindung „Stottern“ (d. h. in Intervallen aktivieren und deaktivieren; fürs mobile Netz geschieht dies durch Umbenennen des APN), wobei (ab der Plus-Version) ausgewählte Anwendungen auch permanente (oder gar keine) Aktivierung für ihre Übertragungen gewährt bekommen können. Wird ein Minimum an Ladezustand unterschritten, kann die App den Netzwerkverkehr auch komplett unterbinden. Ab der Plus-Version ist es überdies möglich, WLAN auch ortsbezogen zu aktivieren.

Bereits die Gratis-Version verspricht eine signifikante Laufzeitverlängerung, mit der Plus-Version sind für ca. zwei Euro die meisten Ansprüche abgedeckt. Für diejenigen, die ein Maximum herausholen möchten, gibt es schließlich die Ultimate-Version für ca. fünf Euro. In allen Fällen wird jedoch die Gratis-Version als „Unterbau“ benötigt: Plus und Ultimate sind lediglich AddOns.



Bild 4.16: *Green Power* macht dem *JuiceDefender* Konkurrenz



Green Power

Als Alternative zu *JuiceDefender* wird häufig **Green Power** (Bild 4.16) genannt – beide Apps sind auch durchaus vergleichbar. Die meisten Dinge werden von beiden Apps gleichermaßen unterstützt, wenn sich ihre Verfügbarkeit auch unterschiedlich auf die Gratis- und

Bezahlversion(en) verteilt. So ermöglicht *Green Power* bereits in der kostenlosen Version, mobile und WLAN-Daten basierend auf Schedule, Display-Status, Ladegerät, Signal-Level und weiteren Kriterien zu steuern (Signal-Level heißt hier: Wird die Verbindung zu schwach, etwa in der U-Bahn, wird sie abgeschaltet und in Intervallen geprüft, ob sich eine Aktivierung wieder lohnt). Dafür sind Widget und Nachtmodus erst in der Bezahlversion (für anderthalb Euro) verfügbar, ebenso wie die Bluetooth-Schaltung. Hinzu kommt in der Premium-Version Unterstützung für *Tasker*, womit sich die fehlende ortsabhängige WLAN-Schaltung und CPU-Steuerung umsetzen ließe, notfalls auch ohne *Green Power*.



SuperPower

Eine automatische Steuerung verspricht auch **SuperPower** (Bild 4.17, in der Notification-Area). Hier werden mobile Daten, WLAN, Bluetooth, CPU (*root*), 2G/3G (*root*), GPS (*root*), AutoSync und Hintergrunddaten (*root*) basierend auf Kriterien wie dem Status von Display / WLAN / LockScreen / Tethering / Schlafmodus / Ladezustand / Batteriestand oder auch Download-Speed und Vordergrund-App gesteuert. Auch diverse Schedules lassen sich nutzen (etwa Nachtmodus, Daten-Stottern). Dinge wie GPS-Kontrolle oder auf Signalstärke basierende Schaltung sind in Planung.



Bild 4.17: Auch **SuperPower** kümmert sich im Hintergrund um verschiedene Sparmaßnahmen

Battery Saver (Bild 4.18) verbindet das automatische Management mit Profilen. So kümmert sich die App beispielsweise im Hintergrund darum, bei zu schwachem Signal WLAN bzw. Radio zu deaktivieren (und periodisch auf Verbesserungen zu prüfen, um es ggf. wie-

der zu aktivieren). Darüber hinaus lassen sich verschiedene Profile (etwa für die Arbeit, zu Hause, draußen ...) mit speziellen Einstellungen für Bildschirmhelligkeit, Klingelton-Lautstärke u. a. m. definieren. Auch das (Ent-)Ladeverhalten lässt sich anhand einer entsprechenden Grafik nachvollziehen.



Battery Saver

Bild 4.18: *Battery Saver* verbindet das automatische Management mit Profilen

Es ließen sich noch eine ganze Reihe weiterer Apps aufzählen, die einzelne Aspekte wie die automatische WLAN-Umschaltung u. a. m. abdecken. In der eingangs genannten Übersicht sind sie aufgeführt – hier würden sie einfach den Umfang des Buches sprengen.

4.4 Platz im internen Speicher schaffen

Aufräumen

Irgendwie naheliegend: Wenn man etwas löscht, wird Platz frei. Besonders geeignete Kandidaten dafür sind Apps, die man ohnehin nicht mehr benötigt – was ja bereits in Abschnitt 4.2 beschrieben wurde (genau wie für root-User das Säubern des Dalvik-Caches). Die Bereinigung von Cache, Chroniken & Co war dort ebenfalls bereits genannt.

Doch so manche App hinterlässt auch nach ihrer Deinstallation noch die eine oder andere Leiche im Keller. Um diese aufzuspüren und zu beseitigen, bietet sich ein Blick auf **SD Maid** (Bild 4.19) an. Damit lassen sich gezielt Rückstände aufspüren und entfernen.



SD Maid

So ganz nebenbei kümmert sich *SD Maid* mittlerweile auch um die anderen gerade genannten Dinge: Installierte Apps lassen sich (zusammen mit dem von ihnen belegten Speicherplatz) auflisten, um unnötige Exemplare zu entsorgen. „Duplicates“ zeigt doppelte Dateien auf. Mit dem „Searcher“ lassen sich Dateien finden, deren Name auf ein bestimmtes Muster passt. Um Cache, Log-Dateien und dergleichen mehr kümmert sich wiederum der „System Cleaner“. *SD Maid* scheint also für den Frühjahrsputz bestens geeignet. Ihr volles Potential kann diese App aber wieder erst mit *root* ausspielen.

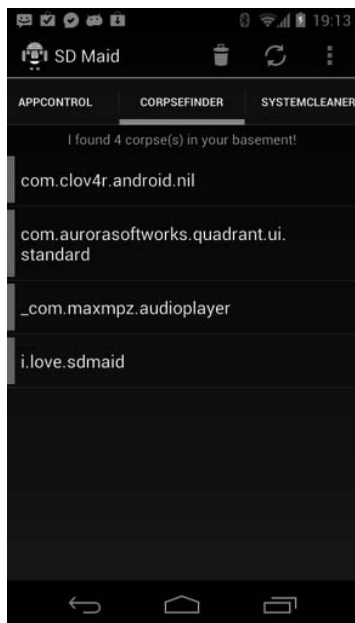


Bild 4.19: *SD Maid* kümmert sich um die „Leichen im Keller“

Auslagern

Genügt das noch immer nicht, stellt man sich oft die Frage: Kann man Apps eigentlich auf der SD-Karte installieren? Oder dorthin auslagern? Ab Android 2.2 (Froyo) ist dies zumindest teilweise bereits von Haus aus möglich. Die Funktionalität nennt sich naheliegenderweise „App2SD“ – muss aber von der jeweiligen App explizit unterstützt werden (andernfalls lässt sich ein Verschieben zwar u. U. erzwingen, aber das kann zu unerwünschten Nebeneffekten führen). Ist dies der Fall, kann man sie aus dem Anwendungsmanager (*Einstellungen* → *Anwendungen* → *Anwendungen verwalten*) mit dem Button *Auf SD-Karte verschieben* auf die selbige befördern. Zumindest teilweise, denn ein gewisser „Grundstock“ verbleibt dabei im internen Speicher. Unter anderem auch der zur App gehörende Dalvik-Cache.

Zwar steht anschließend wieder mehr interner Speicher zur Verfügung, die Sache hat jedoch einen kleinen Haken. Sobald man den Androiden per USB-Kabel an den heimischen Computer anschließt und die Karte an selbigen „freigibt“, steht sie lokal ja nicht mehr zur Verfügung: Vom Androiden aus ist ein Zugriff erst dann wieder möglich, wenn die USB-Verbindung getrennt wurde. Die mit *App2SD* auf die Karte verschobenen Apps können bei am Computer eingebundener SD-Karte also nicht ausgeführt werden. Dies führt insbesondere zu Problemen, wenn Widgets involviert sind, weshalb man Apps mit Widgets besser nicht auf der Karte installiert.

Einige Custom-ROMs bieten daher *App2SD+* an. Dies benötigt allerdings eine eigenständige (zusätzliche) Partition, die mit dem Dateisystem Ext3 versehen sein muss. Wird nun eine USB-Verbindung zum PC hergestellt, verbleibt diese Ext3-Partition beim Androiden. Freigegeben wird lediglich die „herkömmliche“ FAT-Partition. Somit stehen die ausgelagerten Apps weiterhin lokal zur Verfügung.

Ein weiterer Vorteil von *App2SD+* ist, dass auch der Dalvik-Cache mit auf die Karte wandert: Es wird also deutlich mehr Platz freigeschaufelt.

Wer noch auf einer Android-Version vor Froyo fest sitzt oder kein *App2SD+* unterstützendes ROM verwendet, findet in *Link2SD* (Bild 4.20) eine Alternative. Auch diese Lösung benötigt eine separate Partition (es muss jedoch nicht zwingend Ext3 sein – FAT wird von *Link2SD* ebenfalls unterstützt), auf die man sodann die Apps verschieben kann. Im Unterschied zu *App2SD* werden die Apps hier allerdings vollständig auf die Karte befördert und im internen Speicher sodann durch einen passenden symbolischen Link ersetzt. Damit ist die Kompatibilität sichergestellt: Dem System wird so vorgegaukelt, dass sich die ausgelagerte App nach wie vor im internen Speicher befinden würde.



Link2SD



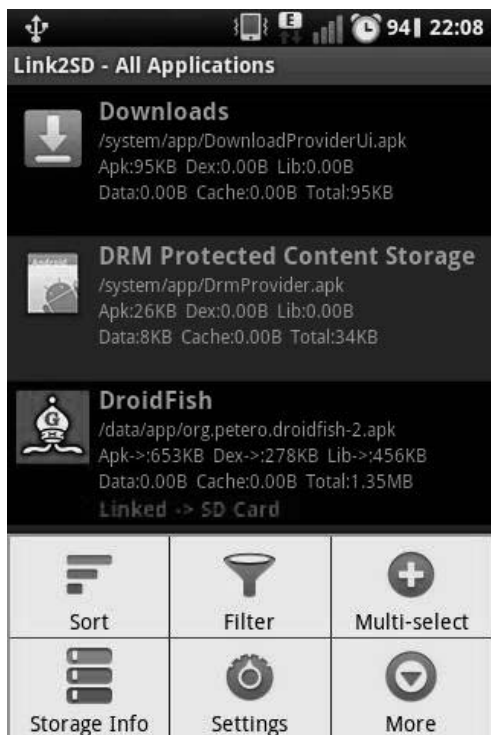


Bild 4.20: *Link2SD* hilft, mehr Platz im internen Speicher zu schaffen

Wie bei *App2SD+* gilt in diesem Falle: Über die USB-Verbindung wird die „App-Partition“ einfach nicht freigegeben, sodass Apps und ihre Widgets weiterhin lokal verfügbar bleiben. Und der Dalvik-Cache lässt sich mit *Link2SD* ebenfalls auslagern, so man dies wünscht.

4.5 Need For Speed

Der Wunsch nach „mehr Speed“ steht in der Regel dem Wunsch nach längeren Akku-Laufzeiten entgegen: Was mehr Leistung bringt, benötigt meist auch mehr Energie. Ausnahmen hiervon sind ein von unnötigen Altlasten befreiter Cache (siehe Abschnitt 4.2 *Cache bereinigen*), die Deinstallation nicht mehr benötigter Apps einschließlich der Beseitigung etwaiger Rückstände (siehe Abschnitt 4.4 *Aufräumen* sowie genügend große Intervalle bei der Synchronisierung der Hintergrunddaten (siehe Abschnitt 4.3 *Hintergrunddaten und Synchronisierung*) – diese Dinge eignen sich für beide Zwecke. Weiteren Punkten wollen wir uns im Folgenden widmen.

RAM bereinigen

Wer bei diesem Thema an Task-Killer denkt, liegt völlig daneben. Task-Killer sind dafür da, Amok-laufende Apps zu beenden, deren man anderweitig nicht habhaft werden kann. Um die Speicher-Bereinigung kümmert sich Android eigentlich selbst recht gut. Zum Verständnis an dieser Stelle ein kurzer Ausflug hinter die entsprechenden Kulissen:

Der Grundgedanke ist, dass das Laden einer App aus dem internen Speicher bzw. gar von der SD-Karte (naturgemäß) zusätzliche Energie benötigt. Ist die App bereits geladen, spart man sich den Ladevorgang. Also versucht Android, einmal geladene Apps im Speicher zu halten, auch wenn der Anwender diese bereits wieder verlassen hat. Da nicht unbegrenzt RAM zur Verfügung steht, kommt dafür ein ausgeklügeltes System zum Einsatz.

Verantwortlich für das Aufräumen ist der sogenannte OOM-Killer (OOM steht für „Out Of Memory“). Steht nicht mehr genügend freier Arbeitsspeicher zur Verfügung, ist der OOM-Killer dafür verantwortlich, welchen zu schaffen – indem er „irgend etwas“ aus dem RAM schmeißt. Für die Auswahl dieses „Verlierers“ werden verschiedene Kriterien verknüpft. Um diesen Vorgang verständlich zu halten, stelle ich das einmal vereinfacht dar:

Zunächst werden im RAM befindliche Prozesse in „Klassen“ eingeteilt. Hierbei erhalten ständig benötigte System-Prozesse eine sehr hohe Priorität. Auf der nächsten Stufe stehen „sichtbare“ Apps (also die, welche der Anwender gerade vor sich sieht, weil er damit arbeitet). Einige „Klassen“ weiter folgen am Ende dann die „leeren“ Apps – das sind die, die vom Benutzer „beendet“ wurden und die keine Tätigkeiten mehr ausführen. Naheliegenderweise wird beim Aufräumen mit der niedrigsten Priorität angefangen. Für die „engere Auswahl“ kommen dann noch weitere Kriterien ins Spiel, die wir an dieser Stelle nicht näher betrachten wollen.

Woher weiß der OOM-Killer nun, wann er tätig werden soll? Dazu sind für jede „Klasse“ Schwellwerte im System konfiguriert. Ein Bild sagt mehr als tausend Worte, und so erklären sich diese Schwellwerte am besten anhand des Screenshots in Bild 4.21, der einen Bildschirm der App **AutoKiller Memory Optimizer** zeigt: Je niedriger die Priorität, desto mehr freies RAM muss verfügbar sein, damit die App geladen bleibt.

Unschwer zu erraten: Diese App ist meine Empfehlung für diesen Zweck. Als Alternative käme **Auto Memory Manager** in Betracht. Beide Apps benötigen root-Rechte, da die genannten Schwellwerte im System verankert sind.

Natürlich gilt es nach Installation der jeweiligen App, die richtigen Einstellungen zu finden. Diese sind natürlich zum einen stark vom Gerät (und dem dort insgesamt vorhandenen RAM) abhängig. Ist weniger RAM verfügbar, fallen auch die Grenzwerte geringer aus. Zum anderen ist da auch noch ein subjektiver Faktor, der nicht verleugnet werden kann. Zum Herantasten bieten beide genannten Apps gute „Presets“

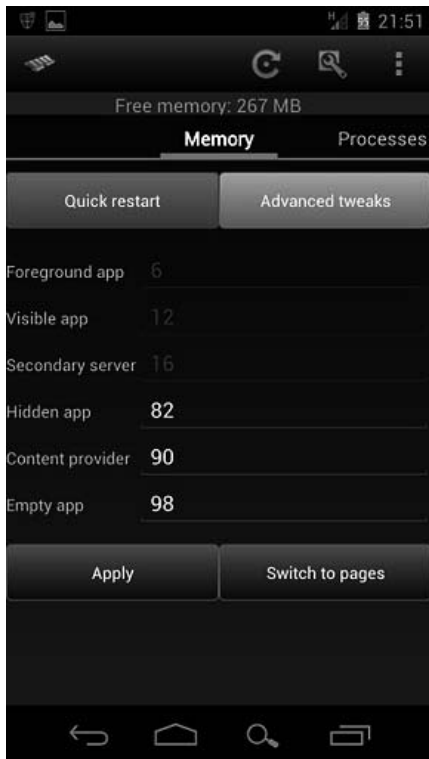


Auto Memory
Manager





(Voreinstellungen) an. Es empfiehlt sich, zunächst mit „Moderate“ (so heißt das entsprechende Preset) zu beginnen und sich von dort aus an die best geeigneten Werte heranzutasten.



AutoKiller Memory Optimizer

Bild 4.21: *AutoKiller Memory Optimizer* hilft beim Feintuning der Grenzwerte für den systemeigenen OOM-Killer



<http://andrs.w3pla.net/autokiller>

Sind die richtigen Werte gefunden, und läuft das System damit flüssig und stabil? Dann weist man im letzten Schritt die ausgewählte App an, diese Werte nach jedem Neustart automatisch zu laden. Aber erst, wenn man sich dessen wirklich sicher ist! Bei zu aggressiven Einstellungen kann das andernfalls zu einem Dauer-Boot-Kreislauf führen, weil beispielsweise das System nach jedem Start gleich wieder „abgeschossen“ wird. Um dies im Ernstfall zu vermeiden, lässt sich zumindest *AutoKiller Memory Optimizer* so konfigurieren, dass die Einstellungen um zwei Minuten verzögert geladen werden. Damit hat man im Ernstfall noch die Möglichkeit einzugreifen. Nebenbei bringt diese App noch etliche weitere System-Tweaks mit, die sich optional aktivieren lassen. Details dazu finden sich auf der **Projektsite**.

Swap-Space nutzen

Unter Windows gibt es hierfür die „Auslagerungs-Datei“, unter Linux richtet man sich am besten eine Swap-Partition ein oder greift, falls man dies bei der Installation vergessen hat und es schnell gehen muss, ebenfalls zu einer Swap-Datei. Was aber hat es mit diesem „Swappen“ oder „Auslagern“ auf sich?

Wird der Arbeitsspeicher (das RAM) knapp, muss Platz geschaffen werden. Im vorigen Abschnitt habe ich erläutert, in welcher Form sich der OOM-Killer um diese Angelegenheit kümmert. Wurde eine App auf diese Weise aus dem RAM entfernt, müssen bei einem Neustart derselben sämtliche benötigten Speicher-Strukturen neu aufgebaut werden. Beim Swappen hingegen wird ein Abbild des entsprechenden Speicherbereiches auf den Datenträger ausgelagert. Ein Neuladen geht auf diese Weise wesentlich schneller und energiesparender vonstatten.

Da böte sich doch eigentlich an, dass dies von Haus aus bereits eingerichtet ist. Wo also ist der Haken? Am Datenträger hängt er. Während bei Desktop-Rechnern „normale Festplatten“ zum Einsatz kommen, verwenden unsere Androiden fast ausnahmslos sogenannten Flash-Speicher. Und der ist hinsichtlich der Schreibzyklen ein wenig empfindlich: Zu viele davon verträgt er nicht. Wer also permanent auf dem gleichen Bereich schreibt (und das ist beim Swapping kaum auszuschließen), verringert damit die Lebensdauer des Datenträgers. Das ist für den einen „schlimm“, der andere hingegen „pfeift darauf“ und kauft sich halt öfter einmal eine neue SD-Karte.

Da es sich hier wieder um einen tiefen Eingriff ins System handelt, bleibt auch diese Tuning-Maßnahme Anwenden mit root-Zugriff vorbehalten. Wer Swap nutzen möchte, dem sei die App **Swapper** (Bild 4.22) ans Herz gelegt.



Swapper

Bild 4.22: *Swapper* hilft beim Einrichten und Verwalten der Swap-Datei





Mit dieser App lassen sich nicht nur alle notwendigen Einstellungen bequem von einer grafischen Oberfläche aus vornehmen, die App kümmert sich auch sonst um alles Nötige. So verringert sie beispielsweise bei entsprechender Konfiguration das Risiko eines schnellen „Aufbrauchens der verfügbaren Schreibzyklen“, indem sie die Swap-Datei bei jedem Neustart an anderer Stelle auf dem Datenträger unterbringt. Im Einzelnen kümmert sich *Swapper* um:

- das Neuanlegen einer Swap-Datei beim Boot (an immer neuen Stellen auf dem Datenträger)
- ein sauberes Abschalten des „Swapping“, wenn der Datenträger per USB gemountet wird
- die Neu-Aktivierung nach Lösen des USB-Mount
- gezieltes Einstellen der „Swap-Prioritäten“

Dies sind nur die wichtigsten Punkte – und jeder davon ist optional. Es lässt sich auch eine Swap-Partition nutzen (das erübrigt dann auch das Abschalten bei USB-Kontakt sowie das spätere Wieder-Aktivieren). In der Regel ist eine Swap-Partition ein wenig schneller als eine Datei, aber aufgrund der begrenzten Schreibzyklen von SD-Karten hat man länger etwas von selbigen, wenn *Swapper* sich darum kümmert, die Datei bei jedem Neustart an anderer Stelle der Karte wieder anzulegen.

Nebenbei: Übertreiben sollte man es auch nicht, ein gutes Mittelmaß ist gefragt. Ist zuviel „Krams“ ausgelagert, bremst das am Ende doch wieder. Gute Anfangswerte sind 32 bis 64 MB Swap sowie eine „Swappiness“ von 10 bis 20.

CPU übertakten

Um das Untertakten der CPU haben wir uns bereits im Abschnitt 4.1 gekümmert – jetzt soll es also in die andere Richtung gehen. Aber auch das funktioniert natürlich nur mit root-Rechten.

Die verfügbaren Mittelchen (auch Apps genannt) sind natürlich die gleichen wie im genannten Abschnitt: *SetCPU* war ja bereits genannt, **CPU-Tuner** (Bild 4.23) ist eine gängige Alternative.

Da es beispielsweise wenig Sinn hat, den Androiden im Leerlauf mit „vollem Speed“ laufen zu lassen (wenn man schläft, hat man daran in der Regel wenig Bedarf), bieten beide Apps auch „Timer“ an sowie die Möglichkeit, unterschiedliche Taktraten für aktiviertes und deaktiviertes Display zu verwenden. Alternativ lassen sich, wie bereits beschrieben, die CPU-Einstellungen auch sehr granular mit *Tasker* vornehmen: So kann man es beispielsweise einrichten, dass beim Start bestimmter ausgewählter Apps die Taktrate der CPU entsprechend angepasst und bei Beendigung/Verlassen derselben der Standard wieder



hergestellt wird. Dies garantiert ein gesundes Mittelmaß zwischen Performance und Akku-Laufzeit, ohne dabei mittelmäßig zu sein.

Vorsicht ist natürlich angesichts der „Obergrenze“ (der höchstmöglichen Taktrate) geboten: Ab einem bestimmten Schwellenwert wird das System instabil. Dann folgen der Kaffeewärmer, der Teekocher und schließlich der Ziegelstein (Brick) – womit das Gerät dann nach Finnland kann. Dort wurde anscheinend die Sportart des Handy-Weitwurfs erfunden. Zumindest gibt es dort seit dem Jahr 2000 die entsprechende Weltmeisterschaft. Der Rekord liegt seit 2005 bei gut 90 Metern.



<http://www.welt.de/reise/article7277909/Handyweitwurf-Frauentragen-Finnland-skuril.html>



CPU-Tuner

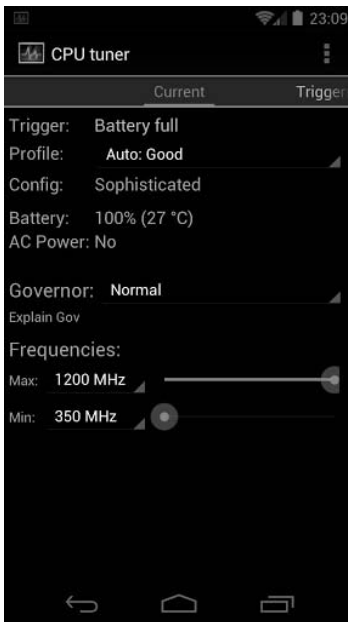


Bild 4.23: Mit *CPU-Tuner* lässt sich die Taktfrequenz der CPU anpassen

A Anhang

A.1 Fragen und Antworten

Bei Woody Allen hieße dieses Kapitel sicher: *Was Sie schon immer zu Android wissen wollten – sich aber nie zu fragen trauten*. Nur keine Hemmungen! Immer her mit den Fragen an Radio Eriwan! Das Prinzip solcher Fragen erklärt der Wikipedia-Artikel zu Radio Eriwan treffend mit einem kurzen Beispiel:

Anfrage an Radio Eriwan:

Stimmt es, dass Iwan Iwanowitsch in der Lotterie ein rotes Auto gewonnen hat?

Antwort:

Im Prinzip ja. Aber ...
 es war nicht Iwan Iwanowitsch, sondern Pjotr Petrowitsch,
 und es war kein Auto, sondern ein Fahrrad,
 und er hat es nicht gewonnen, sondern es ist ihm gestohlen worden.
 Alles andere stimmt.

Jeder wusste, was gemeint war – aber keiner konnte die (versteckte) Kritik am System wirklich „dingfest“ machen. So war der politische Witz im Osten. Und auch wenn sich bei manchen vollmundigen Versprechen der Industrie Größen nicht selten ähnliche Fragen aufdrängen (gesagt wird A, aber jeder weiß, dass eigentlich B dahinter steckt), geht es im Folgenden nicht ganz so wild zu.

Apps & Co.

Was passiert bei Deinstallation einer App mit ihren Daten?

Ganz einfach: Sie werden gelöscht. Alles, was das System der zu deinstallierenden App explizit zuordnen kann, wird mit entfernt. Dazu gehört auch das Verzeichnis, in dem die App ihre Konfigurationsdateien und ggf. Daten (im internen Speicher) abgelegt hat. Auch etliche andere Dateien ließen sich recht einfach zuordnen: Da jede App unter Android einen eigenen „User“ darstellt, lässt sich schließlich ermitteln, welche Dateien ihr gehören.

Eine Ausnahme bildet dabei die SD-Karte: Hier erlaubt das Dateisystem keine Benutzerzuordnung. Daher lassen sich Dateien auf der SD-Karte nicht so leicht zuordnen und bleiben demzufolge meist liegen.



Will Herr oder Frau Poweruser doch einmal eine App deinstallieren und dabei die Daten behalten, lässt sich dies mit Hilfe des SDK erreichen:

```
pm uninstall -k com.app.wegdamit
```

deinstalliert die App mit dem Paketnamen `com.app.wegdamit` – behält (`-k` = „keep“, behalten) aber die Daten auf dem Gerät.

Natürlich hätte man sie auch mit *Titanium Backup* sichern und anschließend wieder herstellen können – *Titanium Backup* fragt ja auch brav: Die App, die Daten oder beides?

Ist das Löschen von Cache und Daten das Gleiche wie Entfernen und Neu-Installation einer App?

Hin und wieder empfiehlt ein Entwickler bei speziellen Problemen mit seiner App diese zu deinstallieren und anschließend neu zu installieren. So manch einer fragt sich: Wäre da das Löschen von Cache und Daten nicht ausreichend? Ist das nicht dasselbe, vom Resultat her?

Ist es nicht. In beiden Fällen werden zwar App-Cache und Daten gelöscht. Bei einer Deinstallation wird aber auch der Dalvik-Cache der App entfernt und bei einer Neuinstallation wieder frisch aufgebaut.

Wo speichert Android die Metadaten zu meinen Fotos?

Was bitte sind Metadaten? Vielleicht sollte das zuerst geklärt werden: Das sind etwa die Stichworte, die man den Fotos zuweisen kann. Und einiges anderes mehr: Welche Covers von Musikalben sich auf dem Gerät finden (und wo), welche Musikalben von welchen Künstlern, Audio-Genres, Playlists, Videos ... Irgendwo muss der Medien-Scanner das ja alles lassen!

Und wo wäre das? Da hierfür der sogenannte *Media Content Provider* zuständig ist, landen die Daten in dessen Datenbanken – die sich unter `/data/data/com.android.providers.media/databases` finden. Und zwar fein getrennt in mindestens zwei Datenbanken: `internal.db` für den internen Speicher und `external-<Geräte-ID>.db` für die jeweilige Speicherkarte. Herankommen tut an diese Dateien natürlich wieder einmal nur Freund *root* – und bei Forensikern erfreuen sie sich besonderer Beliebtheit.



<http://developer.android.com/reference/android/provider/MediaStore.MediaColumns.html>

Wer genaueres zu den Strukturen der in den genannten Datenbanken enthaltenen Tabellen wissen möchte, findet beispielsweise in der *Entwickler-Doku* weitere Angaben – in englischer Sprache, versteht sich.

Wie kann ich eine App im Speicher halten?

Ich benutze App xyz ständig. Doch fast immer, wenn ich zu ihr wechseln möchte, wird sie neu gestartet. Kann ich Android irgendwie dazu bringen, sie im Speicher zu halten?

Diese Frage haben sich die meisten schon einmal gestellt: Warum schließt Android laufend unsere Lieblings-App? Das Prinzip: Wird der Speicher knapp, schlägt der OOM-Killer zu. Mit welcher Wahrscheinlichkeit ihm nun unsere Lieblings-App zum Opfer fällt, hängt unter anderem davon ab, zu welcher „OOM-Klasse“ sie gehört. Ändern kann man diese wieder einmal nur mit *root*.

CyanogenMod bietet zumindest für den Standard-Launcher eine entsprechende Option – aber auch nur für diesen. Dafür kann die App einfach in eine „wichtigere Klasse“ eingeteilt werden, indem ihr `oom_adj`-Wert gesenkt wird. Wie man dies für eine beliebige App erledigen kann, erklärt ein Post bei XDA: Man erstellt eine Datei namens `etc/init.d/99applock` und füllt sie mit folgendem Inhalt:

```
#!/system/bin/sh
sleep 60
PPID=$(pidof com.your.app)
echo „-17“ < /proc/$PPID/oom_adj
renice -18 $PPID
```

`com.your.app` ist dabei mit dem Paketnamen der gewünschten App zu versehen, und `etc/init.d/99applock` mit den passenden Rechten: `chmod 777 etc/init.d/99applock`.



<http://forum.xda-developers.com/showpost.php?p=19766257&postcount=2>

Unterstützen alle Android-Apps NFC?

Das brauchen sie gar nicht – darum sollte sich das System selbst kümmern. Lediglich passende „Intents“ müssen sie bereitstellen, über die sie von außen angesprochen und mit entsprechenden Daten gefüttert werden können (vergleichbar mit APIs). Um das Auslesen und Interpretieren der NFC-Tags kümmert sich der zentrale NFC-Service, der dann auch die passende Aktion auslösen sollte.

Vergleichen lässt sich das am Besten mit den Barcode-Readern, die ja ebenfalls die passende Aktion wählen: So muss etwa die Kontaktverwaltung auch keine Barcode-Unterstützung haben. Erkennt der Barcode-Reader eine Adresse, ruft er die Kontaktverwaltung auf und übergibt ihm diese oder die Telefonnummer an die Telefon-App bzw. die URL an den Web-Browser.

Passende NFC-Apps wären etwa **on{X}** oder **NFC Launcher**. Und natürlich muss auch das Gerät selbst NFC unterstützen.



on{X}



NFC Launcher

Ich habe meinen einzigen Launcher gelöscht!

Die Tücken von root und Custom-ROMs: Einem „normalen Anwender“ dürfte das nicht passieren, da der „Standard Launcher“ im Read-only-Bereich des Systems installiert ist. Ohne Launcher sieht es unter Android natürlich mau aus: Eingehende Anrufe lassen sich zwar noch annehmen, aber man kann keine Apps mehr starten. Wenn das Kind in den Brunnen gefallen ist, gibt es dennoch eine ganz triviale Lösung:

Einfach am PC mit dem Web-Browser den Google Playstore besuchen, sich mit dem auf dem Gerät verwendeten Google-Konto anmelden, sich einen alternativen Launcher aussuchen und die Installation von dort aus anstoßen. Kurz darauf ist wieder ein Launcher verfügbar, und der Androide somit voll einsatzbereit.

Backup & Co.

Hilfe! Ich habe versehentlich etliche (einen ganzen Thread) SMS/MMS gelöscht!

Das passiert leicht: Ein unachtsamer Tapser, und statt einer einzelnen SMS verschwindet gleich der ganze Thread im Daten-Nirvana. Wenn kein aktuelles Backup der SMS-Daten (vgl. Abschnitt 1.1) existiert, sieht es da schlecht aus (und würde ein solches existieren, würde man sicher nicht nach einer Antwort suchen müssen). Gibt es da noch Chancen?

Mit Android < 4.0: Nur für *root*, der über das Custom-Recovery sofort ein Nandroid-Backup anlegt. Mit Android ab Version 4.0 kann man den Schritten in Abschnitt 1.1 unter *Komplett-Backups ohne root* folgen – und hoffen, dass dies die nötigen Dateien enthält.

Diese finden sich nach dem Entpacken der Image-Datei der Datenpartition im Verzeichnis `data/data/com.android.providers.telephony/databases/` (ja, *root* könnte sich dieses auch mit einem Datei-Manager oder per `adb pull` besorgen). Mit einem Programm wie etwa **SqlliteMan** lässt sich nun etwa die im genannten Verzeichnis befind-

liche Datei `mmssms.db` nach den gelöschten Nachrichten durchsuchen. Auch die Datei `mmssms.db-wal` (eine SQLite Journal-Datei – genauer gesagt: Das Write-Ahead-Log) enthält häufig weitere diesbezügliche Daten. Vor dem Bearbeiten mit irgendwelchen Tools legt man sich davon am besten Kopien an – damit man bei einem Fehlschlag nicht wieder ganz vorn anfangen muss.

Ach ja: Genau so funktioniert es natürlich auch mit jeder anderen Datenbank, die eine beliebige andere App in ihrem Datenverzeichnis abgelegt hat.



Die SMS sind noch da – dafür habe ich aber eine Reihe Dateien gelöscht!

Die Dateien waren im internen Speicher? Aha, mit dem root-Explorer gespielt. Dann sollte schnellstens eine Sicherung der Partition durchgeführt werden. Anbieten tun sich hier Nandroid, aber auch dd. Da Letzteres sich für eines der aufgeführten Recovery-Tools besonders gut eignet, dazu ein wenig mehr.

Zuerst muss herausgefunden werden, welche Partition denn benötigt wird. Ist dies nicht bekannt, kann dazu (per ADB oder mit einer Terminal-App) der Befehl `mount` ausgeführt werden. Ohne Parameter aufrufen, zeigt dieser nämlich alle eingebundenen Dateisysteme an. Ich kürze diese Ausgabe hier einmal ein wenig ab:

```
$ mount
<snip>
/dev/block/mmcblk1p26 on /data type ext3 (rw,nosuid,nodev,noatime,nodiratime,errors=continue,data=ordered)
/dev/block/vold/179:1 /mnt/sdcard vfat <snip>
```

Befanden sich die gelöschten Daten also beispielsweise unterhalb von `/data/data`, muss sich hier das Gerät `/dev/block/mtdblock6` gemerkt werden. Des Weiteren ist auch zu sehen, dass sich die SD-Karte unter `/mnt/sdcard` finden lässt – und hoffentlich genügend Platz aufweist:

```
$ df -h /mnt/sdcard /data/data
```

Filesystem	Size	Used	Available	Use%	Mounted on
/dev/block/vold/179:1	14.9G	1.7G	13.2G	11%	/mnt/sdcard
/dev/block/mmcblk1p26	6.5G	382.1M	6.1G	6%	/data

Über 13 GB frei auf der Karte, knapp 7 GB maximal werden benötigt: Passt. Es kann also zur Tat geschritten werden. Bei Aufruf des Befehls `dd` genau auf die Parameter achten! Nicht umsonst wird gemunkelt, „dd“ stünde für „disk destroyer“: Verwechselt man hier die Eingabe und die Ausgabe, ist letztere danach futsch. Also:



```
dd if=/dev/block/mmcblk1p26 of=/mnt/sdcard/data.img
```

Kurz erklärt: „Disk Duplicator, lese von /dev/block/mmcblk1p26 und schreibe alles, was dort ist, nach /mnt/sdcard/data.dd.“ „if“ steht hier also für Eingabe-Datei (englisch „input file“), „of“ für „Ausgabe-Datei“ („output file“). Letzteres ist in unserem Beispiel tatsächlich eine Datei – die Eingabe jedoch ein Gerät. Doch unter Unix/Linux sind auch Geräte Dateien, siehe Wikipedia: *Geräte-datei*.

Zum Retten der Daten wird die SD-Karte an den PC angeschlossen und ein zuvor heruntergeladenes Datenrettungs-Programm darauf losgelassen. Davon gibt es eine ganze Reihe, und drei möchte ich hier auch benennen:

- *Scalpel* gibt es für Linux (bevorzugt), Mac OS X und Windows. Es ist eines der mächtigeren Tools in dieser Klasse – erfordert aber auch ein wenig Eingewöhnung.
- *foremost* gibt es (nur?) für Linux. Da es aber auch mit dd-Images umgehen kann, ist dies für den im obigen Kasten beschriebenen Fall die passende Lösung.
- *TestDisk* unterstützt die größte Anzahl an Betriebssystemen und stellt auch eine menügeführte Benutzeroberfläche bereit.

Details zur Nutzung finden sich auf den Webseiten des jeweiligen Tools.



www.digitalforensicsolutions.com/Scalpel



<http://foremost.sourceforge.net>



<http://www.cgsecurity.org/wiki/TestDisk>

Kann ich Daten aus einem verschlüsselten ADB-Backup extrahieren?

Unter *Komplett-Backups ohne root* in Abschnitt 1.1 habe ich ja beschrieben, wie man ab Android 4.0 auch als „Normalo“ vollständige Backups erstellen kann – Apps und auch ihre Daten. Dabei musste ein Passwort angegeben werden, mit dem das Backup verschlüsselt wird – gegen unbefugte Zugriffe. Die Zugriffe des Eigentümers sind sicher nicht unbefugt (zumindest, wenn es um die Daten geht), aber wie kommt er an sie heran, ohne sie auf dem Androiden wiederherzustellen (und damit aktuellere Daten zu überschreiben)?

Der bereits bei besagtem Backup genannte Ryan Conrad hat natürlich auch dafür eine Antwort parat. Er hat sich eingehend mit dem Thema beschäftigt, da er schließlich dieses Backup/Restore in seinem Programm implementierte. Die einfachste Antwort lautet also: Sein Programm *Droid Explorer* in Version 0.8.8.7 oder höher zu installieren und die gewünschte Datei damit zu entpacken.



Bild A.1: Mit **DroidExplorer** ab Version 0.8.8.7 lassen sich auch verschlüsselte ADB-Backups bequem entpacken

Dieser Tipp gilt zumindest derzeit nur für diejenigen, die Windows auf ihrem Computer einsetzen. Für alle anderen ist ein mögliches Vorgehen auf <http://de.codeplex.com> erklärt. Um wenigstens einen kleinen Anhaltspunkt zu nennen: Die .ab-Datei ist ein mit AES verschlüsseltes Archiv, in dem sich eine TAR-Datei befindet. Und es gibt ein Tool namens *Android Backup Extractor* (kurz: ABE), mit welchem man diesen Tarball aus der .ab-Datei herausholen kann:



<http://de.codeplex.com>

```
java -jar abe.jar unpack <backup.ab> <backup.tar> <password>
```

Da es sich bei ABE also offensichtlich um ein Java-Programm handelt, sollte es auf den meisten Betriebssystemen laufen.



Panik! Nandroid findet kein sd-ext!

Da erstellt man also pflichtbewusst sein Nandroid Backup – und die Bildschirmausgabe endet mit:

```
Backing up system...
Backing up data...
Backing up .android_secure
Backing up cache No sd-ext found. Skipping backup of sd-ext.
Generating md5 sum...

Backup complete!
```

Was heißt hier: No sd-ext found? Habe ich jetzt ein Problem? Ist da etwas „futsch“?

Mitnichten. Das bedeutet lediglich, dass die SD-Karte nicht über eine EXT3- bzw. EXT4-Partition verfügt, die auf diesen Namen hört. Eine solche wurde/wird von verschiedenen Custom-ROMs für ein erweitertes *Apps2SD* verwendet. Gibt es diese Partition also nicht, kommt diese Art von *App2SD* auf dem Gerät wahrscheinlich auch nicht zum Einsatz. Die Meldung ist also kein Grund zur Sorge. Andernfalls würde sie nachdrücklicher zum Ausdruck gebracht und nicht nur „beiläufig ausgegeben“.

Welche Daten sichert eigentlich Google Backup?

Bei der Ersteinrichtung wird man (zumindest ab Gingerbread) ja gefragt, ob man seine Daten bei Google sichern möchte. Was aber wird dabei eigentlich gesichert, wenn man die Frage bejaht?

Ganz offensichtlich sind damit nicht die Kontakte oder Kalenderdaten gemeint – denn die werden auch in die Google-Cloud synchronisiert, wenn man diese Frage verneint. Im Honeycomb User Guide (englisches PDF) heißt es dazu sinngemäß:

- Android Settings, wie WLAN-Netzwerke und Passworte, Benutzerwörterbuch, usw.
- die Einstellungen vieler Google-Apps, wie etwa Browser-Lesezeichen
- die aus dem Playstore heruntergeladenen Apps

Zumindest der letzte Punkt hat wenig Sinn, da diese Informationen ja ohnehin im Playstore hinterlegt sind. Weiter heißt es jedoch, dass auch einige Apps von Drittanbietern diese Backup-Schnittstelle nutzen, um die Daten ihrer Apps zu sichern. Einige, nicht alle.

Wenn man sich nun mit einem neuen bzw. auf Werkseinstellungen zurückgesetzten Gerät erstmalig mit seinem Google-Konto wieder anmeldet, sollen diese Daten wieder hergestellt werden.

Soweit die Theorie. In der Praxis schlägt leider die Wiederherstellung oftmals fehl, wie zahlreiche Berichte zeigen – man sollte sich also keinesfalls auf diese Funktionalität verlassen, zumal der Umfang der gesicherten Daten ohnehin recht eingeschränkt ist.

Rund um die SD-Karte

Warum kann ich App xyz nicht auf die SD-Karte verschieben?

Das kann verschiedene Ursachen haben:

- Die App unterstützt kein *App2SD* (hat der Entwickler so festgelegt). In diesem Fall wird die Option zum Verschieben erst gar nicht angeboten.
- Die App war dort zuvor bereits installiert (und man hat beispielsweise einen Werks-reset gemacht).

Während im ersteren Falle der Entwickler Abhilfe schaffen kann (es sei denn, die App beinhaltet Widgets oder Hintergrund-Dienste – dann darf sie nicht auf die SD-Karte), gilt es in letzterem Falle, selbst Hand anzulegen. Hier sind wahrscheinlich ein paar „Dateileichen“ auf der Karte liegen geblieben – und die müssen weg. Am einfachsten geht das natürlich, wenn man die SD-Karte mit einem Kartenleser an einen Computer anschließt, da Android (ohne root) das entsprechende Verzeichnis „versteckt“ und keinen Zugriff zulässt. Das Vorgehen ist dann etwa folgendermaßen:

1. Den Paketnamen der entsprechenden App ermitteln. Am Einfachsten geht dies, indem man mit dem Web-Browser die App-Seite im Playstore aufsucht, denn dann steht der Paketname in der URL: Unmittelbar hinter dem `id=` (und endet, sobald ein `&` oder `#` auftaucht). Heißt die URL beispielsweise `https://play.google.com/store/apps/details?id=com.rovio.angrybirds&feature=search_result`, so lautet der Paketname `com.rovio.angrybirds`
2. Auf der SD-Karte nach der zugehörigen Datei suchen. Diese befindet sich unter `.android_secure` und hieße in unserem Beispiel höchstwahrscheinlich `com.rovio.angrybirds-1.asec`.
3. Diese Datei löschen.
4. App auf SD verschieben – jetzt sollte es wieder klappen.

Ausführliche Gründe, die eine App für die Installation auf der SD-Karte disqualifizieren, nennt die Android Entwickler-Seite. In der Regel hängt dies damit zusammen, dass die SD-Karte z. B. bei Bereitstellung an einem Computer auf dem Android-Gerät nicht zur Verfügung steht:

- Services: Eine App, die Hintergrunddienste bereitstellt. Diese Dienste stünden dann ggf. nicht zur Verfügung und würden auch nicht automatisch neu gestartet.
- Alarm Services: Registrierte Alarmer würden bei Nichtverfügbarkeit der SD-Karte abgebrochen.
- Live Wallpapers: Könnten ohne die Karte nicht weiterlaufen und würden durch das „Standard Wallpaper“ ersetzt.
- App Widgets: Könnten nicht mehr aktualisiert werden und „verschwinden“ vom Homescreen. Meist sind sie erst nach einem Reboot wieder verfügbar.
- Account Managers: Können bei nicht verfügbarer SD-Karte natürlich auch nicht arbeiten, sind sie auf selbiger installiert. Die damit verbundenen Konten sind daher nicht sichtbar, wenn die Karte „nicht sichtbar“ ist.
- Sync Adapters: Funktionieren nicht, wenn die Karte nicht verfügbar ist.
- Device Administrators: Wären dann ebenfalls außer Funktion, was die Geräte-Funktionalität negativ beeinflussen kann.
- Broadcast Receivers, die auf *boot_completed* lauern: Da dieser Event (*boot_completed*) vor dem Einbinden der Karte gesendet wird, bekommen die auf der Karte installierten Apps davon nichts mit (hier geht es um „nach dem Booten Starten“).
- Copy Protection: Wird Googles Kopierschutz genutzt, kann die betreffende App nicht auf der Karte installiert werden. Googles „Lizenz-Service“ ist davon jedoch nicht betroffen.

Warum kann ich die App xyz nicht updaten?

Sie ist auf der SD-Karte installiert? Ein ähnliches Problem wie das vorige. Aber mit einer anderen Lösung – vorausgesetzt, es ist genügend interner Speicher frei:

1. App in den internen Speicher verschieben
2. Updaten (sollte jetzt funktionieren)
3. App bei Bedarf wieder auf die Karte verschieben

Klingt blöd – klappt aber so.

Muss ich beim Kauf einer SD-Karte auf die „Klasse“ achten?

Das sollte man schon – besonders wenn man auf Performance und Akku-Laufzeit Wert legt. Wer heute eine SD-Karte kauft, sollte nicht aus Geiz-ist-geil-Gründen (Preis) zu einer „Class 2“-Karte greifen – daran hat man wirklich keine Freude. Sie ist recht langsam

(spätestens bei Video-Aufnahmen wird man das deutlich spüren) und im Vergleich mit „höheren Klassen“ auch ein wenig Akku-hungrig.

Eine „Class 4“-Karte dagegen ließe sich bereits als „Budget-Variante“ einstufen, die für viele Einsatzbereiche ausreichend ist – bei Aufnahme von HD-Video könnte es aber auch hier eng werden. Generell empfiehlt es sich daher, noch den einen Euro darauf zu legen und zumindest zu einer „Class 6“-Karte zu greifen. Deren Spezifikationen sollten auch einer HD-Aufnahme Genüge tun.

Schaden tut eine höhere Klasse natürlich nicht – mehr Speed und schonenderer Umgang mit den Ressourcen haben schließlich noch niemanden gestört. Allenfalls der Preis: Je höher die Klasse, desto höherer auch dieser. Doch da liegt die Toleranzgrenze bei jedem anders.

Tuning

Was ist eigentlich „Mobilfunk-Standby“, und warum braucht es so viel Akku?

Hierbei handelt es sich nicht etwa um die „Hintergrunddaten im Standby“, wie ein Post bei den XDA-Developers suggeriert. Vielmehr hat dieser (auf englisch „Cell Standby“ bezeichnete) Zustand direkt etwas mit dem Mobilfunk-Signal zu tun. Oder mit der Abwesenheit desselbigen.

Was passiert, wenn das Signal zu schwach wird? Das Telefon sucht ein neues, stärkeres Signal. Im Regelfall ist ja auch mehr als nur ein Funkmast in der Nähe. Also wird der Antenne mehr und mehr Leistung zugeführt – in der Hoffnung, eine starke und stabile Verbindung gewährleisten zu können. Schließlich will ein Telefon telefonieren, und dazu benötigt es eine Verbindung. Da das System leider nicht intelligent genug zu sein scheint, nach einer angemessenen Zeit dabei eine Pause einzulegen, verbraucht es eben ggf. recht lange Zeit recht viel Strom.

Berichten zufolge fällt dieser zusätzliche Verbrauch bei 4G deutlich höher aus als bei 3G. Und wirft man einen Blick auf die Übersicht der Akkufresser-Daten (*Leistungsaufnahme verschiedener Komponenten*) am Ende dieses Buches, wird klar: 3G frisst sicher noch immer mehr als 2G. Hat man alles gleichzeitig aktiviert, erfolgt die Suche dann auch in allen Bändern (also 2G, 3G und 4G). Daher kann es durchaus sinnvoll sein, sich auf einen Standard festzulegen, wenn man in einem Gebiet mit schlechter Abdeckung unterwegs ist.

Gänzlich vermeiden kann man dieses Problem natürlich, indem man seinen Androiden ausschließlich im Flugzeug-Modus betreibt – was selbstverständlich keine Lösung ist. Einige interessante Apps gibt es jedoch, die in diesem Zusammenhang genannt werden sollten:



<http://forum.xda-developers.com/showthread.php?t=858177>

No Signal Alert protokolliert im Hintergrund, wo man sich in „toten Zonen“ bewegt hat, und kann diese auf einer Karte anzeigen (Bild A.2). Natürlich lässt sich auch die Log-Datei einsehen. Somit weiß man zumindest, wo dieses Unheil droht.



Bild A.2: Mit **NoSignalAlert** lassen sich „Tote Zonen“ mappen

Gleiches weiß auch **OpenSignalMaps** (Bild A.3) zu berichten. Zusätzlicher Nutzen dieser App: Sie zeigt auch an, welche Sendemasten sich in der Nähe befinden. Außerdem bietet sie einen „Kompass“, der die Richtung zur nächstgelegenen starken Zelle anzeigt. Versteht man also seinen Gesprächspartner immer schlechter, kann man sich dank dieser App in die richtige Richtung bewegen, um den Empfang zu verbessern. Auch ein Widget ist hier an Bord. Beide Apps warnen auf Wunsch auch, wenn man eine „tote Zone“ betritt.



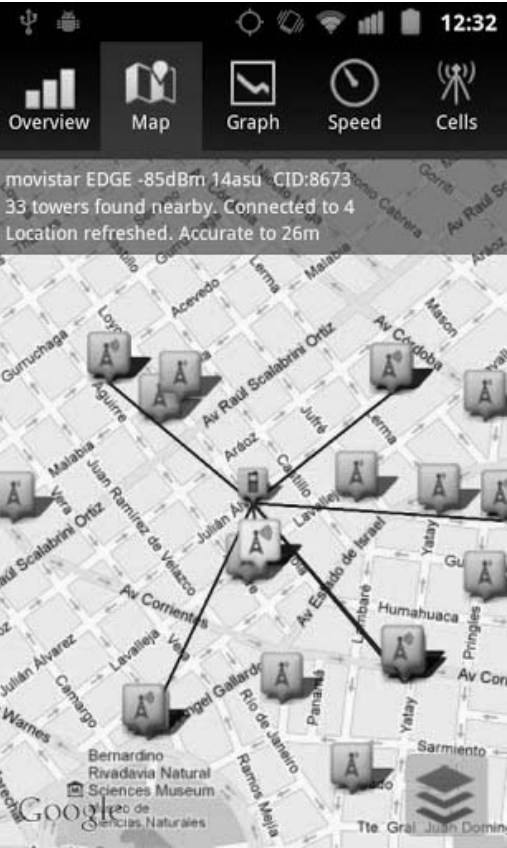


Bild A.3: *OpenSignalMaps* zeigt die nächstgelegenen Mobilfunkzellen auf der Karte an



Network Booster

Den Empfang verbessern möchte hingegen **Network Booster**. Diese App führt einfach einen „Reset“ des Radios durch, wodurch die Netzverbindung frisch aufgebaut wird. Das kann natürlich nur dann etwas bringen, wenn auch (stärkere) Sender in Reichweite sind.

Weitere kleine Helferlein wurden ja bereits in Abschnitt 4.3 benannt.

Ob man davon betroffen ist, lässt sich leicht an den Akku-Statistiken herausfinden (siehe Screenshots Bilder A.4 und A.5). Diese sind in den Systemeinstellungen enthalten, meist unter *Telefoninfo*. Taucht auf der ersten Seite *Mobilfunk-Standby* gleich bei den größten Verbrauchern auf, ist die Wahrscheinlichkeit hoch. Dann einfach die kleine Grafik oberhalb der Werte antippen, was zum zweiten Screenshot führt.

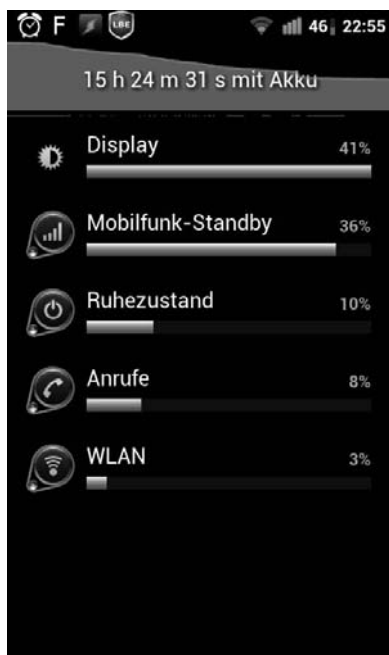


Bild A.4: Akku-Statistiken: Mobilfunk-Standby bei den größten Verbrauchern

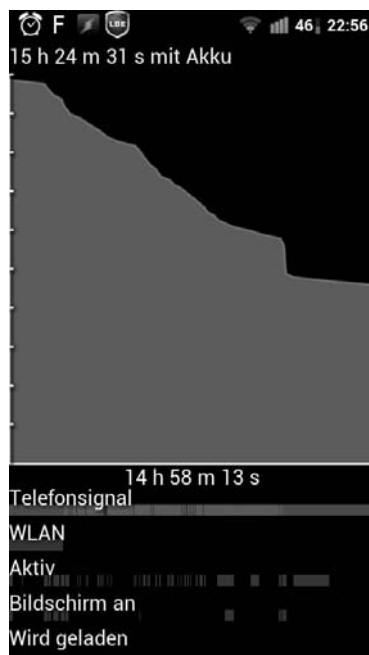


Bild A.5: Die Akku-Statistiken zeigen auch Details zur Qualität des Funksignals

Hier ist der mit *Telefonsignal* beschriftete Balken genauer zu betrachten: Ein kräftiges Grün steht für guten Empfang – was der Verbrauchs-Graph darüber mit einer relativ flachen Kurve als „recht sparsam“ ausweist. Geht der Farbton hingegen ins Gelbliche (mäßiger bis schlechter Empfang) oder wird gar rot (kein Signal), bestätigt auch der Graph darüber einen höheren Stromverbrauch: Die Kurve fällt stärker. Dass dies nicht etwa daran liegt, dass der Anwender gerade viel mit dem Gerät gemacht hat, lässt sich auch erkennen: Der Bildschirm war zu diesen Zeitpunkten (gelblicher bzw. roter Balken) meist ausgeschaltet (keine blaue Markierung bei *Bildschirm an*).

Wie man diesem Problem zu Leibe rücken kann, beschreibt auch der Abschnitt *Akku-Verbrauch im Mobilfunk-Standby mit Tasker bekämpfen* weiter hinten in diesem Buch. Neben *Tasker* werden dabei auch ein paar Alternativen benannt.

Wer frisst meinen Speicherplatz?

Egal, wie groß der Datenspeicher ist – es ist nie genügend davon vorhanden, er ist immer voll. Aber wo ist er abgeblieben? Und wie lässt sich das herausfinden?

Das Menü *Anwendungen* → *Anwendungen verwalten* zeigt zum einen eine „Gesamtzahl“ für belegten und freien Speicher (auf volle Megabytes gerundet). Zum anderen lassen

sich hier die Anwendungen auch nach Größe sortieren, sodass sich besonders speicherhungrige Kandidaten aufspüren lassen.

Auch wenn eine App mit *App2SD* auf die SD-Karte ausgelagert wurde, bleiben noch immer Reste im internen Speicher zurück (ein vollständiges Auslagern ist also nicht möglich).

Temporäre Dateien und Cache belegen Speicherplatz. Letzterer lässt sich problemlos aufräumen (siehe Abschnitt 4.2 unter *Cache bereinigen*) – ersteres ist ein wenig problematischer (siehe unten). Hierzu gehört übrigens auch das Verzeichnis, in dem der Playstore heruntergeladene Dateien vor der Installation zwischenspeichert. So kann es vorkommen, dass dabei die Fehlermeldung über „ungenügenden Speicher“ erscheint, obwohl am Zielort noch genügend zur Verfügung steht: Es ist dann lediglich der „temporäre Speicher“ voll.

Tombstones (so nennen sich bei Android die unter Unix/Linux als *Coredump* bekannten Speicherauszüge, die bei Absturz eines Prozesses angelegt werden können) und System-Log-Dateien belegen ebenfalls Speicherplatz

Kleine Helferlein gibt es natürlich auch hier wieder:



Sandisk Memory Zone

Sandisk Memory Zone zeigt die Kapazitäten (frei/belegt) der verfügbaren Datenspeicher (auch in der Cloud) an und gibt ebenfalls Einblick in Details.

DiskUsage (Bild A.6) erlaubt das Durchwandern der Verzeichnisse nach Dateigröße, womit sich die großen Verbraucher schnell aufspüren lassen sollten.



DiskUsage

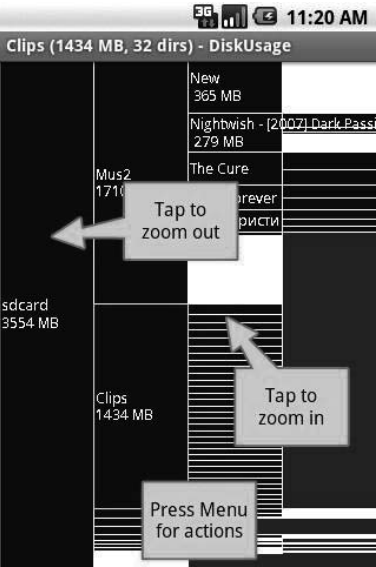


Bild A.6: *DiskUsage* zeigt den Speicherverbrauch grafisch an



Anwender mit root-Rechten haben natürlich wieder einmal weitere Möglichkeiten. Sie können direkt in der Terminal-App (oder via `adb shell`) auf den internen Speicher zugreifen. Um beispielsweise die fünf „größten Brocken“ auf der Daten-Partition aufzuspüren, würde sich etwa folgender Befehl eignen: `su -c „du /data“ | sort -rn | head -n 5`.

Auf gleiche Weise lassen sich natürlich auch die übrigen Dateisysteme erkunden. Welche es gibt, verrät u. a. ein `df -h`, das nebenbei auch noch die aktuellen Größenordnungen (freier und belegter Speicher) in gut lesbarem Format anzeigt.

Verschiedenes

Warum werden neue Medien nicht angezeigt?

Ich habe gerade eine ganze Reihe (Bilder / Videos / MP3-Dateien) per WLAN auf mein Android-Gerät kopiert. Warum zeigt (die Galerie / die Video-App / die Musik-App) nichts davon an?

Damit die genannten Apps nicht bei jedem Aufruf erst alle Verzeichnisse nach Medien durchsuchen müssen, hat man sich bei Android etwas Schlaues einfallen lassen: Den *Medien-Scanner*. Dieser wird bei bestimmten Ereignissen automatisch vom System aufgerufen und durchsucht sodann den gesamten Speicher. Was er dabei findet, wird in eine Datenbank eingetragen. Somit können Apps wie die Galerie oder Video-/Musik-Apps einfach auf diese Datenbank zurückgreifen. Das geht wesentlich schneller und spart obendrein auch noch Akku.

Der Haken ist: Bei welchen Ereignissen tritt der *Medien-Scanner* denn in Aktion? Die Antwort: nach dem Systemstart und nach dem Einbinden der SD-Karte. Punkt. Nicht nach dem Kopieren über das WLAN.

Abhilfen mit Bordmitteln wären hier:

- Das Gerät neu starten. Kein toller Vorschlag – klappt aber.
- Die SD-Karte kurz aus- und wieder Einhängen. Geht über die Systemeinstellungen: *Speicher* → *Speicherkarte entnehmen* – ist aber auch umständlich.
- Abwarten, bis der *Medien-Scanner* aus einem anderen Grund anspringt – dauert viel zu lange.

Eine einfache Abhilfe findet sich natürlich wieder einmal im Playstore, in Form von kleinen Apps wie **Rescan SDCard!**. Diese kann man als Shortcut auf dem Homescreen ablegen und so mit einem einfachen Antippen starten. Die App macht dann nichts anderes, als dem *Medien-Scanner* Bescheid zu geben: Aufwachen, es gibt etwas zu tun! So tritt dieser sofort in Aktion.



Rescan SDCard!

A.2 Begriffserklärungen

ADB

Die Android Debug Bridge ist Bestandteil des Android-SDK. Anders als der Name es nahelegt, ist ADB für mehr als nur das Debuggen gut. So lässt sich hiermit ein Android-Gerät steuern und kontrollieren, Dateien können übertragen, installiert oder auch gelöscht werden und mehr. Eine genauere Beschreibung findet sich auf der Entwicklerseite.



[http://developer.
android.com/tools/
help/adb.html](http://developer.android.com/tools/help/adb.html)

AES

AES ist der Nachfolger des Verschlüsselungs-Standards DES – und bringt als solcher natürlich eine vergleichbar höhere Sicherheit mit.

AOSP

Hinter dieser Abkürzung verbirgt sich das Android Open Source Project – also die Kern-Entwicklung des Android-Systems, auf der alle weiteren Android-Entwicklungen (inklusive der Hersteller-spezifischen „Dreingaben“ wie TouchWiz, MotoBlur, Sense & Co., aber auch die meisten CustomROMs) aufbauen.

API

Kurzform (oft gesprochen, wie man es schreibt, aber auch als Abkürzung buchstabiert) steht für Application Programmers Interface. Gemeint ist hier eine definierte Schnittstelle, über die Informationen bezogen werden können. Die Android-API bietet auf diese Weise z. B. Informationen über den Akkustand und Anderes mehr. So muss nicht jeder Programmierer das Rad neu erfinden.

APK-Datei

Die Abkürzung steht für Android Package, und darin befindet sich in der Regel eine App zur Installation unter Android. Da diese Apps ja in Java geschrieben sind, verwundert es sicher nicht, dass das APK-Format eine „Abwandlung“ des JAR (Java ARchive) ist und sich somit mittels WinZip & Co. ein Blick in selbige werfen lässt.

Datei-Manager unter Android erkennen diese Packages natürlich und bieten an, die enthaltene App zu installieren.

APN

Kürzel für Access Point Name (zu Deutsch: Name des Zugangspunktes). Gemeint ist in der Praxis mitnichten nur der Name, sondern vielmehr der komplette Datensatz.

App

Kurzform für Application. Wird auch im Deutschen („Neudeutsch“: Applikation) verwendet, da „Anw“ einfach blöd klingt. Denn nichts anderes bedeutet das englische Wort Application: Anwendung.

Im Zusammenhang mit Smartphones aller „Couleur“, also Früchte wie auch KGMs (kleine Grüne Männchen), hat sich die Kurzform „App“ eingebürgert – „Application“ (oder im Deutschen „Anwendung“) wird hier eher selten verwendet.

Baseband

Oh oder auch „Radio-ROM“ bzw. „Radio-Image“ wird es gern genannt. Das ist quasi die eigentliche Geräte-Firmware. Hat weniger direkt mit Android als vielmehr mit der Hardware zu tun und initialisiert letztere, so dass sie von ersterem genutzt werden kann. Also sowas Ähnliches wie das BIOS beim PC. Und genau wie dieses befindet es sich i.d.R. auf einem separaten Chip.

Das Teil bootet also die Hardware und übergibt dann an den eigentlichen Bootloader, der sich um Android kümmert.

Bloatware

Vom Hersteller oder Provider vorinstallierte Software, die nicht jedermann benötigt (beispielsweise die Aktien-App). Der Begriff leitet sich vom englischen Wort „to bloat“, „aufblähen“, ab, da diese Apps das ROM unnötig „aufblähen“. Aufgrund der Tatsache, dass sie im ROM integriert sind, kann ein Anwender sie ohne root-Zugriff nicht entfernen.

Bootloader

Sozusagen der „zweite Teil“ nach dem Baseband (daher auch „SPL“ oder „Secondary Program Loader“ genannt). Bleiben wir weiter bei den Hinke-Vergleichen, sind wir hier etwa im „Boot-Manager“ (Lilo, Grub) gelandet (davor wäre noch der „MBR“ oder „Master Boot Record“ auf dem PC – das wäre hier der „IPL“, der „Initial Program Loader“ – der ist bei Androiden in Hardware gegossen und daher nicht veränderbar).

Aber das wäre jetzt nur sehr grob und ungenau, denn es steckt mehr darin: der Android-Bootloader sowie weitere Boot-Optionen wie das Recovery-Menü, Fastboot u.a.m.

Brick

In der Regel das Lebensende eines Androiden – der dann nur noch als Briefbeschwerer oder Ähnliches erhalten kann. Wörtlich heißt das zwar „Ziegelstein“, aber das würde im Deutschen u. U. zu Verwechslungen mit gewissen Androiden aus dem Hause Motorola führen ...

Was sich Google dabei dachte, als es die gleichnamige Permission einführte, sei der Fantasie überlassen (vgl. letzten Abschnitt in Anhang A.3).

Wie verwandelt man einen Androiden nun in einen „Brick“? Dazu werde ich hier keine Schritt-für-Schritt-Anweisung geben (da wenig sinnvoll). Nur soviel sei gesagt: In etwa 95% aller Fälle hängt das mit dem Flashen eines zum Gerät inkompatiblen RUU zusammen. Vermeiden lässt sich solches also durch gründliches Lesen der Anleitungen und Prüfen des „Zubehörs“ vor dem „Brutzeln“.

CalDAV

CalDAV steht für Calendaring Extensions to WebDAV und bezeichnet den nach **RFC 4791** spezifizierten Zusatz, der einen Zugriff auf Kalenderdaten über WebDav ermöglicht.



<http://tools.ietf.org/html/rfc4791>

CSV

Diese Abkürzung steht für den englischen Begriff Comma Separated Values. Er beschreibt das Format einer reinen Textdatei zur Speicherung einfacher Tabellendaten.

Custom-ROM

Ein Custom-ROM ist eine alternative Firmware, mit der man das vorinstallierte Android-System ersetzen kann – wenn man über root-Rechte auf dem Android-Gerät verfügt. Custom-ROMs sind oftmals speziell auf die entsprechenden Geräte angepasst und bieten in der Regel einen Mehrwert, etwa eine aktuellere Android-Version, als der Hersteller sie anbietet. Oder weniger „Zwangsbeglückungen“ (vorinstallierte Apps, die sich nicht ohne weiteres entfernen lassen). Auch zusätzliche Funktionalitäten sind hier keine Seltenheit.

Dalvik

Dafür muss ich ein klein wenig ausholen: Android besteht, vereinfacht gesagt, aus einem Linux-Kernel, auf dem eine spezielle Java-Version läuft. Letzteres ist die sogenannte Dalvik VM (wobei „VM“ für „Virtual Machine“ steht). Android Apps sind also in Java geschrieben.

Für die Ausführung der App wird der Java Code in einen sogenannten „Byte Code“ übersetzt, der optimal auf die Hardware (und die Android-Version) angepasst ist. Damit dies nicht bei jeder Ausführung der App geschehen muss, passiert diese „Übersetzung“ unmittelbar nach der Installation der App – und der Byte-Code wird im sogenannten Dalvik Cache abgelegt. Da dies nach der Installation eines „neuen Systems“ für alle Apps geschehen muss, dauert auch der erste Start nach der Neuinstallation ein wenig länger (dafür geht die Ausführung der Apps nachher entsprechend schneller).

Bei der Installation eines neuen ROMs muss aus genannten Gründen (optimale Anpassung ans System) der Dalvik Cache neu aufgebaut werden. Dafür gibt es im Recovery-Menü einen extra Menüpunkt, aber das ist im entsprechenden Kapitel erklärt.

Debuggen

Wörtlich „entkäfern“. Ein Computer-antiker Begriff, der noch aus einer Zeit stammt, in der „Programmierung“ durch das Ziehen von Drähten, Stecken von Röhren und Löten von Leiterbahnen stattfand. Da war der „Bug“ im „Programm“ nämlich durchaus wörtlich zu nehmen – wenn ein verbrutzelter Käfer für einen Kurzschluss sorgte.

Die Käfer sind mittlerweile zu groß geworden (oder vielmehr die Chips zu klein), trotzdem haben sich beide Begriffe gehalten: „Bug“ für einen Fehler im Programm und „Debuggen“ für die Suche nach und das Entfernen desselben.

DES

DES steht für Data Encryption Standard. Es handelt sich dabei um einen symmetrischen Verschlüsselungsalgorithmus, der 1976 als offizieller Standard der US-Regierung bestätigt und seither international vielfach eingesetzt wird.

DHCP

Die Abkürzung steht für das Dynamic Host Configuration Protocol, welches in vielen Netzwerken zum Einsatz kommt. In WLANs ist es fast immer in Verwendung. Meldet sich ein Gerät beim DHCP-Server an, erhält es von diesem die für die Netzwerk-Kommunikation notwendigen Konfigurations-Parameter: Eine eigene IP-Adresse, die Adresse des zuständigen Routers, Nameserver usw.

DNS

Das Kürzel steht für das Domain Name System. Vereinfacht gesagt, handelt es sich dabei um eine Art „Telefonbuch“ für das Internet, mit dem sich Domain- oder Rechner-Namen wie beispielsweise `www.google.com` in „Anschluss-Nummern“ (die hier „IP-Adressen“ heißen) wie in diesem Beispiel `209.85.148.104` übersetzen lassen.

eMMC

Eine emulierte MultiMediaCard: Gibt sich quasi als SD-Karte aus – tatsächlich handelt es sich jedoch um NAND-Flash.

Fastboot

Der Name ist zunächst ein wenig irreführend, handelt es sich hier doch nicht um die Möglichkeit, das Android-Gerät schneller einsatzbereit zu haben. Fastboot hat eigentlich mit dem installierten Android-Betriebssystem nicht einmal direkt etwas zu tun.

Zu finden ist ein Fastboot-Eintrag gelegentlich im Boot-Menü. Und gedacht ist es in erster Linie zum schnellen Bearbeiten von Partitionen via USB. Dazu wählt man am Android-Gerät diesen Punkt aus und kann dann vom PC aus mit der entsprechenden Software passende Befehle absetzen – etwa um die Daten auf einer Partition zu löschen, mit einer Image-Datei zu überschreiben oder schlicht das Gerät neu zu starten.

Flashen

Den Androiden mit einem neuen ROM versehen – sei es ein „offizielles Firmware-Update“ oder ein Custom-ROM. Der Name rührt daher, dass hier die Daten größtenteils im „internen Speicher“, dem sogenannten „Flash Speicher“, landen.

FTP

Das File Transfer Protocol dient, wie der Name es sagt, der Übertragung von Dateien im Netz. Es gilt für diesen Einsatzbereich als besonders effizient und ressourcenschonend.

GPG

GNU Privacy Guard (GPG) ist ein auf OpenPGP basierendes Kryptographiesystem, welches u. a. RSA-Schlüssel empfiehlt und verwendet.

GPS

Das Global Positioning System wird genutzt, um per Kreuzpeilung verschiedener Satelliten den aktuellen Standort in bis zu vier Dimensionen zu bestimmen: Länge, Breite, Höhe und Zeit.

Hardreset

Auch Rücksetzen auf Werkseinstellungen genannt: Wiederherstellung des Auslieferungszustandes. Stimmt natürlich nicht so ganz, denn die ursprüngliche Firmware wird dabei nach einem Update nicht wieder hergestellt; es werden lediglich alle Nutzerdaten einschließlich vom Anwender installierter Apps etc. gelöscht.

HTTP

Hinter dieser Abkürzung verbirgt sich das HyperText Transport Protocol, das zur (unverschlüsselten) Übertragung von Webseiten z. B. mit Web-Browsern verwendet wird. Erkennbar meist daran, dass die Adresse mit `http://` beginnt.

HTTPS

Klingt so ähnlich wie der vorige Punkt – und ist es auch: Das HyperText Transport Protocol Secure tut das Gleiche – nur eben verschlüsselt, also für sicherere Übertragung. Erkennt man dann daran, dass die Adresse im Browser mit `https://` beginnt.

iCal

Gemeint ist hier das auf vKalendar basierende Datenformat ICalendar. Dieses dient zum Austausch von Kalenderinhalten und ist in *RFC 5545* standardisiert.



<http://tools.ietf.org/html/rfc5545>

IMEI

Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät eindeutig identifiziert werden kann. Diese Nummer ist also Gerätespezifisch und wird von diversen Werbe-Modulen gern zur Identifizierung herangezogen. Mit ihr lässt sich aber auch ein Gerät beim Netzanbieter sperren, sodass ein Dieb es nicht mehr verwenden kann (zumindest nicht im gesperrten Netz – dies weltweit durchzusetzen, dürfte ein wenig aufwendig sein).

IntraNet

Ein privates, i. d. R. lokal begrenztes Netzwerk. Abgeleitet vom lateinischen „intra“ („innerhalb“) und dem englischen „net“ (Netzwerk), da es sich meist um ein firmeninternes Netz handelt.

Kernel

Da steckt das Wort „Kern“ drin, genau. Wenn wir hier vom „Kernel“ sprechen, meinen wir den „Betriebssystem-Kern“, den „Linux-Kernel“. Das ist, vereinfacht ausgedrückt, eine Abstraktions-Schicht: Unten speziell an die jeweilige Hardware angepasst, stellt der Kernel „oben“ eine einheitliche Schnittstelle (API) für die Software zur Verfügung.

Bei Android läuft auf dem Linux-Kernel die Dalvik-VM (eigentlich je eine pro App) und in der Dalvik-VM sodann die App.

KML

Die Keyhole Markup Language ist ein spezieller XML-Dialekt, der zum Austausch geografischer Informationen verwendet wird. Die bekanntesten Vertreter, die dieses Format verwenden, sind Google Maps und Google Earth. Eine Spezialform davon ist KMZ: Hier steht das „Z“ für „ZIP“, die Datei ist also komprimiert. Auf diese Weise ist es möglich, zusätzliche Elemente wie Icons mit der KML-Datei beisammen zu halten.

MAC-Adresse

Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient. Bei Apple wird sie auch Ethernet-ID, Airport-ID oder Wi-Fi-Adresse genannt, bei Microsoft Physikalische Adresse. (*Wikipedia*)

NAND-Flash

Daraus besteht der interne Speicher unserer Androiden: Flash-Speicher, der in der sogenannten NAND-Technik gefertigt ist.

Nandroid-Backup

Ein vollständiges System-Backup, welches sich z. B. aus dem Recovery-Menü heraus erstellen und auch wieder herstellen lässt. Hier werden nicht einzelne Dateien gesichert,

sondern ein Abbild („Image“) des gesamten Systems wird angelegt. Es ist also ein „Alles-oder-Nichts“: Die Wiederherstellung einzelner Dateien ist hier nicht vorgesehen (auch wenn dies mit *Titanium Backup* mittlerweile möglich ist).

Insbesondere bevor man ein Custom-ROM einspielt, aber auch generell vor einem System-Update sollte ein Nandroid-Backup angelegt werden. Es ist natürlich auch sonst immer eine gute Idee, ein komplettes Backup zur Hand zu haben.

NAS

Network Attached Storage oder stark vereinfacht ausgedrückt: Festplatte mit Netzwerk-Anschluss „for the Housegebrauch“. Mittlerweile gibt es NAS-Systeme mit einer Kapazität von 2 TB bereits für weniger als 200 Euro.

NFS

Wie der Name es vermuten lässt, erlaubt das Network File System den Dateizugriff über das Netzwerk – ähnlich wie bei einer Windows-Laufwerks-Freigabe. Dieses Protokoll kommt hauptsächlich unter Linux/Unix zum Einsatz.

Notification Area

Die Notification Area ist auch als „Statusbereich“ bekannt und wird durch die Statusleiste am oberen Bildschirmrand repräsentiert. Zieht man diese Leiste nach unten, öffnet sich die „Area“ mit detaillierteren Informationen, die Apps dort hinterlegen können.

OOM-Killer

Der Name lässt etwas „Böses“ vermuten – doch der Benannte sorgt für Stabilität: Es handelt sich um den System-Prozess, der – sobald der Arbeitsspeicher (RAM) knapp wird (OOM: Out Of Memory) – wieder für Platz sorgt, indem er „Altlasten“ entsorgt: Apps, die nur im Hintergrund rumliegen und länger nicht mehr benutzt oder gar vom Benutzer bereits beendet wurden beispielsweise. Mit root-Rechten ausgestattet, kann man auch konfigurieren, wie viel Platz er mindestens freihalten soll.

OTA

Da liegt was in der Luft ... Denn OTA steht für „Over The Air“. Ja was denn? Beim Rundfunk ist es „On The Air“ und heißt Musik. Bei Phil Collins „In The Air Tonight“. Und bei Android ein „(komplettes) Over The Air Update“ – also ein Kotau, sozusagen.

Die Frage wäre nur, wer der Kaiser ist ... Also, kurz gefasst: Beim OTA werden Software-Updates des Herstellers/Providers über das Funknetz des Letzteren verteilt.

Partition

Eine Partition ist ein zusammenhängender Bereich auf einem Datenträger (unter Windows häufig mit einem Laufwerksbuchstaben verbunden).

Auf einem Android-System sind immer mehrere Partitionen in Benutzung, auch wenn nur der interne Speicher zur Verfügung steht (und keine SD-Karte eingelegt ist): So ist das „/system“ in der Regel nur lesend eingebunden (um Änderungen im Betrieb zu verhindern), während für Apps und Daten eine eigene Partition („/data“) bereitsteht.

Die SD-Karte beinhaltet meist nur eine (in der Regel unter „/sdcard“ eingebundene) Partition. Es sind aber auch hier mehrere Partitionen möglich (und werden z. B. mit App2SD+/Link2SD auch verwendet) – wobei Android bei Anschluss an den PC via USB nur jeweils die erste Partition davon freigibt.

Peer-to-Peer

Das englische Wort „peer“ bedeutet soviel wie „Gleichgestellter“. Teilnehmer in einem Peer-to-Peer-Netzwerk sind sich also „gleichgestellt“ – im Gegensatz zu einem „Client-Server-Modell“. Jeder Teilnehmer kann also sowohl Dienste eines anderen in Anspruch nehmen als auch eigene Dienste bereitstellen.

Permission

...meint hier die im Android-System definierten Zugriffsberechtigungen, wie im Abschnitt 1.2 unter *Zugriffsrechte* erklärt. Eine Übersicht dazu findet sich im Anhang A.3 *Google Permissions*.

Proxy

Ein Vermittler (von lateinisch proximus, der Nächste). Gemeint ist hier ein Service, der ihm übergebene Anfragen weiterleitet – da sie beispielsweise auf direktem Wege nicht zustellbar sind. Denkbare ist auch, dass ein Proxy Daten für den schnelleren Zugriff optimiert – meist indem er selbige zwischenspeichert („caching proxy“). Er könnte aber auch, wie im Falle des Web-Browsers Opera oder des „Mobilizers“ von Google, Bilder für mobile Geräte herunterrechnen, um so den Traffic zu minimieren (und die Übertragung zu beschleunigen).

RAM

Diese drei Buchstaben stehen für Random Access Memory – also Speicher, auf den man nach Belieben an beliebiger Stelle zugreifen kann. Im Gegensatz nicht etwa zu ROM, sondern zu Dingen wie Bandlaufwerken (jaja, so alt ist der Begriff schon), bei denen man sich erst mühsam vom Start zur gewünschten Position (linear) vortasten muss.

Sowohl auf PCs wie auch auf unseren Androiden ist damit meist der Arbeitsspeicher gemeint, in den die Programme/Apps zur Ausführung geladen werden. Üblicherweise ist dies der Bereich, der generell zu klein ist oder von dem man nie genug haben kann ...

Recovery-Menü

Ein separater Bereich des Boot-Menüs, aus dem heraus verschiedene Operationen wie Nandroid-Backup oder auch das Bereinigen des Dalvik-Caches möglich sind.

In das Recovery-Menü gelangt man in der Regel durch eine spezielle Tasten-Kombination beim Einschalten. Diese ist aber zumindest von Hersteller zu Hersteller unterschiedlich. Bei HTC ist es üblicherweise das Halten der „Leiser-Taste“ während des Einschaltens. Bei Motorolas Milestone muss die Kamera-Taste beim Einschalten gedrückt gehalten und anschließend die „Lauter-Taste“ betätigt werden. Und so weiter. Bei Bedarf also am besten im Forum erlesen/erfragen.

Reguläre Ausdrücke

Ein regulärer Ausdruck lässt sich am besten als Zeichenkette mit Suchmustern beschreiben. Dank komplexer Regeln lässt sich damit recht gezielt auch in größeren Textmengen suchen.

ROM

Richtig offensichtlicher Mist ist diese real offerierte Mehrdeutigkeit: Manchmal hat man den Eindruck, er wurde nur zur Verwirrung der Massen eingeführt. Wer einmal den Namen für eine Android-Komponente nicht kennt, sagt einfach „ROM“. Klingt, als wüsste man voll Bescheid – und die Chance, dass das auch noch Sinn ergibt, ist verdammt hoch.

Aber im Ernst: Worum geht es hier? Eigentlich steht der Begriff „ROM“ für Read Only Memory – also Speicher, auf den ausschließlich lesend zugegriffen werden kann. Ja, richtig: So wie bei CD-ROM, da steckt das ja auch drin. Nur bei Android, da kann das alles Mögliche sein. Nicht selten sachlich falsch – aber wen kümmert's? Schauen wir uns also die einzelnen Bedeutungen einmal an:

Systemspeicher: Teile des Android-Systems werden in der Tat „nur lesend“ eingebunden. Unter anderem eine Schutzmaßnahme, um Veränderungen zu erschweren (damit wir die

dusseligen Apps, mit denen uns die Hersteller/Provider „beglücken“, nicht einfach löschen können). So heißt es z. B. in den Spezifikationen des HTC Wildfire: „384 MB RAM; 512 MB ROM“. Nonsens(e): Ein Blick hinter die Kulissen offenbart, dass nur 250 MB read-only (/system) eingebunden sind. Die restlichen 250 MB „ROM“ stehen zur Installation von Anwendungen zur Verfügung. Read-only? Mitnichten. De facto kann der ganze Bereich jederzeit schreibbar gemacht werden, sofern man *root* hat. Also eher irreführend – richtiger müsste es hier heißen: „interner Speicher“, oder – in Abgrenzung vom RAM – „interner Flash-Speicher“.

Das System selbst: Um die Verwirrung komplett zu machen, wird auch hier gern von „ROMs“ gesprochen. Das hat schon Tradition: Auch bei älteren Spiele-Konsolen sprach man davon, „ein ROM zu laden“. Hier war es aber „seinerzeit“ tatsächlich eine Cartridge – also ein Speicher-Chip, den man an das Gerät steckte. Später kamen dann die Emulatoren, welche die „antiken Geräte“ auf moderner Hardware emulieren können. Und hier kommt diese „Cartridge“ natürlich in Form einer Datei daher. Den Begriff „ein ROM laden“ hat man beibehalten. Und schließlich weiter übertragen ...

root

Aus Herstellersicht: Die Wurzel allen Übels. Objektiv betrachtet: Der Administrator (auch „SuperUser“) eines Linux-Systems. Er darf alles und kann alles (kaputtmachen auch, ja).

RSA

RSA ist ein asymmetrisches kryptographisches Verfahren, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann (Wikipedia). Hierbei kommt ein Schlüsselpaar (privater und öffentlicher Schlüssel) zum Einsatz. Der Name des Verfahrens setzt sich aus den Anfangsbuchstaben der Familiennamen seiner Erfinder zusammen: Rivest, Shamir, Adleman.

RUU

Radio Unit Update: Eine Art *update.zip* für das Radio-Image, also ein „Firmware-Upgrade“.

ROM Upgrade Utility: Wie der Name bereits sagt, ein Utility zum Upgrade des ROM, das entweder vom Hersteller oder von Drittanbietern zur Verfügung gestellt und vom PC aus installiert wird.

Wenn nicht ganz klar ist, was von beidem gemeint ist, ist es in der Regel das erste – wobei das durchaus mit dem zweiten identisch sein kann, da die Begriffe oftmals gleichbedeutend verwendet werden. Was mancherorts als „ROM Upgrade Utility“ bezeichnet wird, ist nämlich nichts anderes als das Update des Radio-Images.

Salt

Salt (deutsch: Salz) bezeichnet in der Kryptographie eine zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung als Eingabe einer Hashfunktion angehängt wird, um die Entropie der Eingabe zu erhöhen. (*Wikipedia*)

SDK

Das SDK ist die Grundlage für die Android-App-Entwicklung und liegt für die jeweilige Version von Android vor. Es ist aber nicht nur dafür verwendbar, sondern bringt auch einige brauchbare Tools wie Fastboot, den Dalvik Debug Monitor sowie ADB mit.

Ergänzt man das Ganze noch um Eclipse, kann es mit der Entwicklung von Apps losgehen!

SIP

Das Session Initiation Protocol findet in der Internet-Telefonie häufige Anwendung, und wird im allgemeinen Sprachgebrauch teilweise gar mit „VoIP“ (Voice-over-IP, also der Internet-Telefonie selbst) gleichgesetzt.

SMB

Server Message Block (kurz SMB, teils auch als LAN-Manager- oder NetBIOS-Protokoll bekannt) ist ein Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Netzwerken. Es ist der Kern der Netzwerkdienste von Microsofts LAN-Manager, der Windows-Produktfamilie sowie des LAN-Servers von IBM. Weiter wird es von den frei verfügbaren Softwareprojekten Samba und Samba-TNG verwendet, um Windows-Systemen den Zugriff auf Ressourcen von UNIX-basierten Systemen zu ermöglichen und umgekehrt. (*Wikipedia*)

Unter Linux/Unix wird das Kürzel übrigens mit zwei Vokalen angereichert, damit man es leichter aussprechen kann: SaMBa.

Sniffer

Ein Sniffer (engl. to sniff, riechen, schnüffeln) ist eine Software, die den Datenverkehr eines Netzwerks empfangen, aufzeichnen, darstellen und ggf. auswerten kann. Es handelt sich also um ein Werkzeug der Netzwerkanalyse. (*Wikipedia*)

SSH

Das Kürzel SSH bezeichnet die Secure Shell, was zum einen ein Netzwerk-Protokoll, zum anderen aber auch entsprechende Programme für die Herstellung/Nutzung einer sicheren Datenverbindung benennt. Es kommt i. d. R. eine starke Verschlüsselung zum Einsatz, die auch bereits beim Verbindungsaufbau und der Anmeldung (Login) gilt.

SSI

Server-Side Includes bezeichnet einfache, i. d. R. in HTML-Dokumente eingebettete Skript-Befehle, welche der Web-Server vor der Auslieferung der Seite an den Client interpretiert und durch entsprechende Inhalte ersetzt.

SSID

Diese Abkürzung steht für den Begriff Service Set Identifier und bezeichnet den frei wählbaren Namen eines WLAN-Netzes.

Symlink

Eine symbolische Verknüpfung, auch symbolischer Link, Symlink oder Softlink genannt, ist eine Verknüpfung in einem Dateisystem (Dateien und Verzeichnisse), die auf eine andere Datei oder ein anderes Verzeichnis verweist. Es ist also lediglich eine Referenz auf die Zieldatei bzw. das Zielverzeichnis. (*Wikipedia*)

Tethering

Das Bereitstellen einer bestehenden Netzverbindung für andere Geräte. In unserem Kontext handelt es sich dabei in der Regel um eine mobile Datenverbindung, die per WLAN, Bluetooth oder USB weitergegeben wird.

TAR

Kurzform für Tape Archive – denn dafür wurde dieses Format ursprünglich eingesetzt. Obwohl Bandlaufwerke heutzutage weitgehend zum „alten Eisen“ gehören, ist das Format (zumindest in der Unix- und Linux-Welt) nach wie vor sehr beliebt – und kommt meist in Verbindung mit einem Kompressionsprogramm wie GZip oder BZip daher.

TOR

Das hat jetzt nichts mit Fußball zu tun, und ich bin auch nicht Balla-Balla. Wer genau hinschaut erkennt, dass alle drei Buchstaben groß geschrieben sind – ganz offensichtlich handelt es sich hier also um eine Abkürzung.

Und die steht für The Onion Router. Gedacht ist hier an die unzähligen Schalen oder Schichten, die eine Zwiebel hat (und vielleicht auch an die Tränen, die ein Auseinandernehmen derselben verursacht). Beim TOR-Netzwerk steht jede Schicht hier für eine Erhöhung der Anonymität: Je mehr Router beteiligt sind, desto schwieriger lässt sich der Absender eines Paketes ausmachen.

Traces

Die Ablaufverfolgung (englisch tracing) bezeichnet in der Programmierung eine Funktion zur Analyse oder Fehlersuche in Programmen. [...] Dabei wird z. B. bei jedem Einsprung in eine Funktion sowie bei jedem Verlassen eine Meldung ausgegeben, sodass der Programmierer mitverfolgen kann, wann und von wo welche Funktion aufgerufen wird. (Wikipedia)

Tracker

Tracker leitet sich vom englischen Wort „track“, also „Spur“ ab. Ein Tracker in unserem Kontext versucht, Nutzerspuren aufzuzeichnen. Klassische Beispiele sind die Web-Bugs. Nicht verwechseln: Im Bereich „GPS & Navigation“ gibt es auch „Tracker“, die Spuren aufzeichnen – hier ist das aber definitiv gewünscht, um anschließend z. B. die zurückgelegte Route auf einer Karte ansehen zu können.

Tunnel

Ein Tunnel bündelt die Netzwerk-Kommunikation eines oder mehrerer Protokolle und bettet diese ggf. in ein anderes Protokoll ein. Am Tunnelein- und -ausgang wird dabei das „originale Protokoll“ (z. B. HTTP zum Abruf einer Webseite) benutzt, während die Übertragung im Tunnel verschlüsselt (beispielsweise über SSH) abläuft.

Update.Zip

Ganz offensichtlich eine Datei. Und ebenso offensichtlich will sie etwas aktualisieren – nur was? Es handelt sich hier um ein „flashbares Update“. Offizielle Firmware-Updates kommen meist unter diesem Namen daher. Und da das System eine Datei, so sie im Wurzel-Verzeichnis der SD-Karte liegt, als ein solches betrachtet, lässt sich auf diese Weise

auch so einiges anderes ins System mogeln. Das nutzt z. B. *Titanium Backup* aus, wenn es ein `update.zip` erstellt.

Einspielen lässt es sich zum Beispiel über das Bootmenü.

VNC

Virtual Network Computing, kurz VNC, ist eine Software, die den Bildschirminhalt eines entfernten Rechners (Server) auf einem lokalen Rechner (Client) anzeigt und im Gegenzug Tastatur- und Mausbewegungen des lokalen Rechners an den entfernten Rechner sendet. Damit kann man auf einem entfernten Rechner arbeiten, als säße man direkt davor. (*Wikipedia*)

VPN

Ein Virtuelles Privates Netzwerk bindet einen Computer (oder, in unserem Fall, einen Androiden) über eine verschlüsselte Verbindung in ein entferntes Netzwerk (Firmennetz, Uni-Netz, heimisches Netzwerk) ein, als wäre er „dort vor Ort“.

Web-Bug

Kleine Wanzen, die sich auf diversen Webseiten verstecken, um Besucher-Informationen zu sammeln. Mancherorts werden sie auch verharmlosend „Zählpixel“ genannt.

Man mag sich fragen: Welchen Schaden kann so ein 1x1 Pixel großes Bildchen denn anrichten? Kommt ganz darauf an. Denn beim Abruf desselbigen vom Server wird ja nicht nur diese kleine Grafik-Datei zum Benutzer übertragen. Auch in der Gegenrichtung fließen so einige Informationen: Auf welcher Webseite war das Bild eingebunden (Referrer)? Welche IP-Adresse/Browser/Betriebssystem/... hat der Anwender im Einsatz? Wo war er noch (Kekse/Cookies helfen gern dabei, Lücken zu schließen).

WebDAV

WebDAV steht für **Web-based Distributed Authoring and Versioning** und ist ein offener Standard zur Bereitstellung von Dateien im Internet, über den auf Daten wie bei einer Online-Festplatte zugegriffen werden kann. Dabei ist auch eine Versionskontrolle spezifiziert. In der Regel wird WebDAV über einen Web-Server umgesetzt, da es sich hier um eine Erweiterung des HTTP-Protokolls handelt.

Wipe

Wörtlich übersetzt: Löschen. Das „Was“ ist hier allerdings die Frage. Und da kommt es darauf an, wen man fragt bzw. wie man den Wipe initialisiert.

Hardreset: Eine Form des Wipe ist mit diesem gleichbedeutend, denn sie löscht lediglich die „/data“-Partition. Das ist der Bereich, in dem die selbst installierten Apps sowie die Daten abgelegt werden.

Dalvik-Cache: Mit dem Wipe/Löschen des Dalvik-Caches erzwingt man eine Neu-Übersetzung des Programmcodes aller Apps. Damit geht kein Datenverlust einher: Lediglich der nächste Gerätestart dauert etwas länger.

Komplett-Wipe: Den gibt es in verschiedenen Versionen des Recovery-Menüs. Sollte nur ausgeführt werden, wenn man auch wirklich weiß, was man da tut: Er löscht nämlich alle Daten von allen Partitionen, auch von „/system“. Danach geht dann nichts mehr – es lässt sich lediglich ein neues ROM einspielen.

XML

Die eXtensible Markup Language stellt hierarchisch strukturierte Daten in Form von Textdaten dar und wird u. a. für den plattform- und implementationsunabhängigen Austausch von Daten zwischen Computersystemen eingesetzt. Normalerweise enthalten XML-Dateien keinen Binärcode, auch wenn dies aufgrund der Erweiterbarkeit durchaus möglich ist. Daher kann man selbige notfalls auch im „Texteditor“ betrachten – wenn auch nicht unbedingt sehr komfortabel.

A.3 Google Permissions – und was sie bedeuten

Normalerweise sieht man eine Kurzbeschreibung der Permission (z. B. bei der Installation einer App). Die technische Bezeichnung taucht selten im Klartext für den Anwender auf – man kann aber z. B. auch einen Blick auf das *Manifest* werfen, und da stehen sie im Klartext.

Nun werde ich aber hier nicht alle Permissions auflisten, das wäre einfach zu viel. Man findet sie bei Interesse im Entwickler-Handbuch (allerdings auf Englisch). Ein paar ausgewählte, die doch häufiger einmal auftauchen könnten, möchte ich aber hier kurz erklären:



http://de.wikibooks.org/wiki/Googles_Android/_Das_Manifest



<http://developer.android.com/reference/android/manifest.permission.html>

Permission	Erklärung
ACCESS_COARSE_LOCATION	Ungefährer (netzwerkbasierter) Standort. Hier kommt kein GPS zum Einsatz, sondern die Informationen von Funkmasten (Cell-ID) sowie WLANs
ACCESS_FINE_LOCATION	Genauer (GPS-) Standort. Exakte, per GPS ermittelte Standortdaten.
ACCESS MOCK_LOCATION	Falsche Standortquellen für Testzwecke. Fake Location (falsche Standortdaten vom System anfordern). Für Testzwecke gedacht (z. B. im Emulator); wird aber auch benötigt, um ein externes GPS Gerät nutzen zu können. Hier geht es nicht darum, einer anderen App eine Fake-Location unterzujubeln – das ginge allenfalls in Verbindung mit INSTALL_LOCATION_PROVIDER.
ACCESS_NETWORK_STATE	Netzwerkstatus anzeigen. Informationen über Netzwerke (besteht eine Verbindung, und wenn ja zu welchem Netzwerk?)
ACCESS_SURFACE_FLINGER	Zugriff auf die API des „Surface Flinger“ (Teil des Medien-Frameworks unter Android: Stellt einen systemweiten „Oberflächen-Kompositor“ bereit, der sich um das Rendering in Framebuffer-Devices kümmert - also Grafik, Grafik-Beschleunigung und so).
ACCESS_WIFI_STATE	WLAN-Status anzeigen. Informationen über WiFi-Netzwerke (besteht eine Verbindung, und wenn ja zu welchem Netzwerk? Welche Netzwerke sind verfügbar?)
ACCOUNT_MANAGER	Als Konto-Manager fungieren. App darf mit Konto-Authentifizierern interagieren. (für Systemanwendungen reserviert).
AUTHENTICATE_ACCOUNTS	Als Kontoauthentifizierer fungieren. Konto-Authentifizierungsfunktionen verwenden, Konten erstellen, Abrufen und Einstellen der zugehörigen Passwörter.
BIND_APPWIDGET	Widgets auswählen. Erlaubt einer App dem AppWidget-Service mitzuteilen, welche App auf die AppWidget-Daten zugreifen darf. Mit dieser Berechtigung kann anderen Anwendungen Zugriff auf persönliche Daten gewährt werden. Laut API-Referenz sollten nur sehr wenige Apps diese Permission benötigen.
BLUETOOTH	Bluetooth-Verbindungen herstellen. Zugriff auf bereits „autorisierte“ Bluetooth-Geräte

Permission	Erklärung
CLEAR_APP_USER_DATA	Alle Cache-Daten der Anwendung löschen. Benutzerdaten beliebiger/aller Apps löschen (siehe Einstellungen-Anwendungen verwalten, der Button „Daten löschen“ bei jeder Anwendung) – richtiger wäre also Anwendungsdaten löschen oder CLEAR_APP_DATA, das „User“ verwirrt hier ein wenig.
DELETE_CACHE_FILES	(einzelne) Dateien aus dem Cache löschen
DELETE_PACKAGES	Anwendungen löschen. Apps entfernen/löschen/deinstallieren/wegmachen
DEVICE_POWER	Tiefgreifender (low-level) Eingriff in die Energieverwaltung (Power Management). Hat nicht direkt etwas mit „Power Off“ zu tun, könnte aber bei Missbrauch durchaus zu selbigem führen...
DIAGNOSTIC	Lese-/Schreibberechtigung für zu Diagnosegruppe gehörige Elemente. Lese- und Schreibzugriff auf „diagnostic resources“ – die API-Referenz beschreibt leider nichts Genaueres.
DISABLE_KEYGUARD	Tastensperre deaktivieren. Tastensperre (inkl. deren Passwort-Schutz) deaktivieren, sodass der Bildschirm nicht mehr automatisch gesperrt wird. Sinnvoll z. B. bei Video-Apps und insbesondere bei Navis – und bei eingehenden Telefonaten.
EXPAND_STATUS_BAR	Statusleiste ein-/ausblenden. Status-Bar (Notification?) erweitern/kollabieren. Wohl die Lite-Version von STATUS_BAR
GET_ACCOUNTS	Bekannte Konten suchen. Liste konfigurierter Accounts abrufen (nur die Accounts, nicht die Zugangsdaten selber). Mit dieser Permission kann lediglich festgestellt werden, welche Accounts existieren.
GET_TASKS	Laufende Anwendungen abrufen. Informationen über laufende Anwendungen abrufen. Wird natürlich von Task-Managern und -Killern, aber auch von Akku-Statistik-Apps benötigt. „Böse Apps“ können dies nutzen, um auszukundschaften, wo sich lohnende Daten zum Klauen finden lassen.
INJECT_EVENTS	Tasten und Steuerungstasten drücken. „Generieren“ und „Ausführen“ bestimmter Events, wie z. B. Benutzer-Eingaben. Die App kann also vermutlich andere Apps „fernbedienen“.

Permission	Erklärung
INSTALL_ LOCATION_ PROVIDER	App will selber Ortsdaten bereitstellen („Du bist jetzt hier“). Woher sie die nehmen will? Naja, vielleicht von einem Bluetooth-GPS o.ä.
INSTALL_ PACKAGES	Anwendungen direkt installieren. Andere Apps installieren. Kann OK sein (App-Manager), muss aber nicht (Wallpaper etc. wollen vielleicht eher Schadsoftware nachladen, wenn sie diese Permission anfordern)
INTERNET	Uneingeschränkter Internetzugriff. Öffnen von Netzwerk-Sockets. Die App kann also beliebige Internet-Verbindungen herstellen. Wird von allen Apps gebraucht, die Werbung anzeigen wollen – aber auch von Web-Browsern, Mail-Apps, u. a. m..
KILL_ BACKGROUND_ PROCESSES	Alle Anwendungen im Hintergrund schließen. Hintergrund-Prozesse „töten“, also beenden. Dabei kann es sich um die eigenen Prozesse handeln (was dem Anwender die Möglichkeit gibt, das Programm tatsächlich zu beenden, statt es nur in den Hintergrund zu schieben) – es können aber eben so gut fremde Prozesse beendet werden. I. d. R. handelt es sich dann um einen Task-Manager oder Task-Killer.
MANAGE_ ACCOUNTS	Als Konto-Manager fungieren. Accounts/Zugangsdaten verwalten – also auch verändern. Die Doku ist leider wieder einmal sehr vage – aber hier würden bei mir die Alarmglocken läuten.
MODIFY_PHONE_ STATE	Telefonstatus ändern. Status der Telefonie anpassen: Power, MMI-Codes (z. B. Rufumleitung [de]aktivieren, Rufnummernübermittlung ein/ausschalten) etc. – jedoch nicht Anrufe tätigen. Allerdings kann das Netzwerk (zu einem anderen Anbieter, Roaming) gewechselt oder die Mobilfunkverbindung ein- bzw. ausgeschaltet werden, ohne dass der Benutzer davon informiert wird.
MOUNT_FORMAT_ FILESYSTEMS	Externen Speicher formatieren. Externe Dateisysteme (SD-Karten etc.) formatieren (Vorsicht! Nach dem Formatieren ist das entsprechende Dateisystem leer, die (vorher) darauf befindlichen Daten sind weg!). Nix für Wallpaper, Spiele etc.!

Permission	Erklärung
MOUNT_ UNMOUNT_ FILESYSTEMS	Dateisysteme bereitstellen oder Bereitstellung aufheben. Dateisysteme ein- und ausbinden. Toll für externe Festplatten am Telefon – gilt aber ebenso für SD-Karten.
PROCESS_ OUTGOING_ CALLS	Abgehende Anrufe abfangen. Ausgehende Anrufe beobachten, verändern oder abbrechen. Hm, könnte das einen Anruf bei der Mailbox ins Ausland weiterleiten? A propos Mailbox: Eine entsprechende Permission für eingehende Anrufe konnte ich bislang nicht entdecken.
READ_CALENDAR	Kalenderdaten lesen. Sollte klar sein: Alle Termine können damit gelesen werden.
READ_CONTACTS	Kontaktdaten lesen. Damit ist das Adressbuch fällig.
READ_FRAME_ BUFFER	Zugriff auf die Frame-Buffer Daten (vereinfacht gesagt: Den Inhalt des Bildschirms). Erlaubt u. a. das Erstellen von Screenshots. Da stellt sich die Frage: Warum gibt es dann keine App zur Erstellung von Screenshots, die keine root-Rechte benötigt?
READ_HISTORY_ BOOKMARKS	Erlaubt lesenden Zugriff auf Lesezeichen und Browserverlauf (Chronik).
READ_LOGS	System-Protokolldateien lesen. Lesender Zugriff auf die Log-Dateien des Systems. Hier werden allgemeine Informationen zu durchgeführten Aktionen gespeichert, i. d. R. jedoch keine vertraulichen Informationen (es sei denn, ein Programmierer hat etwas verbockt).
READ_OWNER_ DATA	Eigentümerdaten lesen. Auslesen der auf dem Gerät gespeicherten Eigentümerdaten.

Permission	Erklärung
READ_PHONE_STATE	Telefonstatus lesen und identifizieren. Zugriff auf die Telefonfunktionen des Gerätes. Eine Anwendung mit dieser Berechtigung kann unter anderem die Telefon- und Seriennummer dieses Telefons ermitteln und feststellen, ob ein Anruf aktiv ist oder mit welcher Nummer der Anrufer verbunden ist. Ein Media-Player kann so z. B. bei eingehenden Anrufen automatisch auf „Pause“ schalten (dafür benötigt er diese Permission aber nur unter Android 1.6 oder früher – ab Version 2.0 gilt diese Ausrede nicht mehr). Bei Werbung (z. B. AdMob) wird dies häufig zum Auslesen der IMEI/IMSI genutzt, um festzustellen, welche Werbung auf dem Gerät bereits angezeigt wurde (eindeutige Identifizierung, Tracking). Bei Apps, die auch für Android 1.6 und früher kompatibel sein sollen, wird diese Permission automatisch gesetzt.
READ_SECURE_SETTINGS	Lesezugriff auf Systemeinstellungen (u. a. Umschalter für die mobile Datenverbindung). Eigentlich dem System vorbehalten.
READ_SMS	SMS oder MMS lesen. Damit lassen sich bereits gespeicherte Kurznachrichten lesen. Darunter können natürlich auch vertrauliche Informationen sein.
READ_SYNC_SETTINGS	Synchronisierungseinstellungen lesen. Lesezugriff auf die Einstellungen der Synchronisation – etwa um festzustellen, ob selbige für Kontakte aktiviert ist. Ein gutes Zeichen: Die App möchte vielleicht wissen, ob der Anwender eine Datensynchronisation im Hintergrund erlaubt, und sich (hoffentlich) entsprechend verhalten.
READ_SYNC_STATS	Synchronisierungsstatistiken lesen. Beispielsweise den Verlauf bereits durchgeführter Synchronisationen einsehen.
REBOOT	Erlaubt den Neustart des Gerätes. Wie der Name es bereits andeutet: Diese App kann mal eben einen Reboot veranlassen.
RECEIVE_BOOT_COMPLETED	Automatisch nach dem Booten starten. App möchte benachrichtigt werden, wenn der Bootvorgang abgeschlossen ist. I.d.R. heißt das: Sie möchte nach dem Booten automatisch gestartet werden. Manchmal darf der Anwender dabei aber auch über die Konfiguration der App entscheiden, ob sie das dann wirklich tut.

Permission	Erklärung
RECEIVE_MMS, RECEIVE_SMS	MMS empfangen, SMS empfangen. Eingehende MMS/SMS abfangen – da möchte wohl jemand mitlesen. Kann aber durchaus OK sein, wenn die App auf MMS/SMS reagieren soll. Auf der anderen Seite kann man damit eingehende Nachrichten auch „im Nirvana“ verschwinden lassen...
RECORD_AUDIO	Audio aufnehmen. Tonaufnahmen erstellen. Das kann sowohl für ein „Diktaphon“ genutzt werden – als auch zum Mitschneiden von Telefonaten.
RESTART_PACKAGES	Anwendungen neu starten. Laufende Apps neu starten. Wird z. B. verwendet, um von selbigen ein Backup erstellen zu können. (In der API-Referenz mittlerweile auf „deprecated“ gesetzt, sollte also in neueren Versionen nicht mehr genutzt werden)
SEND_SMS	Kurznachrichten senden. Und zwar ohne Zutun des Benutzers, auch an richtig teure Premium-Dienste (womit klar ist, wozu „böse Apps“ das gern hätten). Es gibt aber auch „gute“ Gründe für diese Permission: Natürlich die SMS-Apps, aber teilweise auch In-App-Käufe, die nicht über Google Checkout abgewickelt werden.
SET_ACTIVITY_WATCHER	Die Ausführung von Systemaktivitäten beobachten. Wird meist für Debugging benutzt. Wenn es also keine Beta ist, hat der Entwickler vielleicht nur vergessen, das wieder raus zu nehmen.
SET_ALWAYS_FINISH	App kann sich selber beenden – also wirklich beenden, nicht nur in den Hintergrund gehen.
SET_ANIMATION_SCALE	Allgemeine Animationsgeschwindigkeit einstellen. Anpassung der Animationsgeschwindigkeit (schnellere/langsamere Animationen).
SET_PREFERRED_APPLICATIONS	App kann jeder Aktivität eine Default-App zuweisen (etwa den Browser zum Öffnen einer URL). In neueren Android-Versionen ohne Auswirkung.
STATUS_BAR	Kann die Status-Bar (Notification?) öffnen, schließen und ausblenden. Meist will die App wohl Letzteres, um einen „Vollbild-Modus“ zu ermöglichen.

Permission	Erklärung
SUBSCRIBED_FEEDS_READ	Abonnierte Feeds lesen. Abrufen von Details zu den derzeitig synchronisierten Feeds.
SUBSCRIBED_FEEDS_WRITE	Abonnierte Feeds schreiben. Änderungen an kürzlich synchronisierten Feeds vornehmen.
SYSTEM_ALERT_WINDOW	Warnungen auf Systemebene anzeigen. Fenster mit Systemwarnungen einblenden. Eine böswillige App kann so den gesamten Bildschirm blockieren. Sollte eigentlich nicht benutzt werden, da dies für System-Meldungen gedacht ist. Erlaubt das Anzeigen von „Alert Windows“, d. h. Nachrichtenfenstern, die immer im Vordergrund angezeigt werden.
USE_CREDENTIALS	Authentifizierungsinformationen eines Kontos verwenden. Möchte die konfigurierten Zugangsdaten verwenden. Das heißt nicht unbedingt, dass es sie „zu sehen bekommt“ – aber die App kann sich quasi „im Namen des Anwenders“ anmelden.
USE_SIP	App kann Internet-Telefonie nutzen (SIP ist das gebräuchlichste Protokoll dafür)
VIBRATE	Vibrationsalarm steuern. Wird gern genutzt, um beispielsweise auf die Beendigung (oder auch den Start) einer Aktivität hinzuweisen – oder generell, um die Aufmerksamkeit des Anwenders zu wecken. Laute Töne sind ja nicht immer erwünscht. „Vibrieren“ heißt: Lass das Gerät zittern und summen...
WAKE_LOCK	Standby-Modus deaktivieren. App kann das System daran hindern, einen Ruhezustand einzunehmen (also den Bildschirm zu dimmen, die CPU „schlafen“ zu lassen etc.) Wäre doch blöd, wenn die Navi-App läuft und plötzlich der Bildschirm ausgeht.
WRITE_APN_SETTINGS	Einstellungen für Zugriffspunktname schreiben. App kann die Zugangsdaten zum Internet etc. (siehe <i>Begriffserklärung APN</i>) verändern. Meist geht es der App nur darum, den Namen des APN zu ändern – um die Verwendung des mobilen Datenverkehrs zu steuern (Beispiel: <i>APNDroid</i>).

Permission	Erklärung
WRITE_CALENDAR	Kalenderdaten schreiben. Diese Permission erlaubt lediglich den Schreib-, nicht aber den Lesezugriff auf den Kalender. Die damit versehene App kann also Termine hinzufügen, nicht aber lesen oder ändern.
WRITE_CONTACTS	Kontaktdaten schreiben. Wie WRITE_CALENDAR, nur in Bezug auf die Kontaktdaten bzw. Browser-History (Chronik) und Lesezeichen.
WRITE_EXTERNAL_STORAGE	App darf beliebige Daten auf der (externen) SD-Karte lesen, schreiben, verändern und auch löschen – prinzipiell auch die Daten anderer Apps. Diese Permission ist aber beispielsweise essentiell für diverse Backup- und Kamera-Apps, die natürlich Daten auf der Karte manipulieren müssen.
WRITE_OWNER_DATA	Eigentümerdaten schreiben. Schreiben/verändern der auf dem Gerät gespeicherten Eigentümerdaten.
WRITE_SECURE_SETTINGS	Allgemeine Systemeinstellungen ändern. Lesen und Schreiben von Systemeinstellungen. „Secure Settings“ können nur von Systemanwendungen (also solchen, die ins „ROM“ integriert wurden) angefordert werden.
WRITE_SYNC_SETTINGS	Synchronisierungseinstellungen schreiben. Schreibzugriff auf die Einstellungen der Synchronisation. Eine mit dieser Permission ausgestattete App kann u. a. die Synchronisation von Kontakten und Kalendern aktivieren bzw. deaktivieren.
com.android.vending.BILLING	In-App Payment (in der App integrierte Bezahldienste, die über den Google Playstore abgewickelt werden)

Weniger gebräuchliche sowie offensichtlich klingende Permissions (Was heißt wohl *BRICK*? Ja, genau: Phone in Sachen Brauchbarkeit mit einem Ziegelstein vergleichbar zu machen, also unbrauchbar. Nicht lachen – diese Permission gibt es wirklich!) habe ich hier ausgelassen; die müssen also bei Bedarf im Entwickler-Handbuch selber nachgeschlagen werden. Oder man wirft einen Blick auf die App *AllPermissions* (bei AndroidPIT – aus dem Google Playstore wurde sie entfernt). Wie der Name bereits suggeriert, handelt es sich hier um eine dummy-App, die alle (unter Android 2.1 verfügbaren) Permissions verlangt. Da AndroidPIT hier bei „Mouse Over“ kurze Erklärungen anzeigt, lernt man dabei auch einiges.



<http://www.androidpit.de/de/android/market/apps/app/youten.redo.allpermission/AllPermissions>

A.4 Akkuverbrauch im Mobilfunk-Standby mit Tasker bekämpfen

Unter *Was ist eigentlich „Mobilfunk-Standby“, und warum braucht es so viel Akku?* wurden ja bereits die Hintergründe des *Mobilfunk-Standby* und seines Energieverbrauchs erklärt. Der Kernpunkt dabei war, dass bei schlechtem oder gänzlich abhanden gekommenem Funksignal zusätzliche Energie aufgewendet wird, um wieder eine gute Verbindung herzustellen. Was natürlich wenig Sinn hat, wenn man in einem Funkloch sitzt. In diesem Kapitel wollen wir nun betrachten, was sich dagegen unternehmen lässt.

Dazu habe ich mir zunächst einige Apps angeschaut, die das Problem bekämpfen wollen. Die Erfolge waren recht durchwachsen, doch zwei Apps schlugen sich recht gut. Zum einen ist dies die abgebildete App *Autopilot*, und zum zweiten das ebenfalls abgebildete *NoBars*.



Autopilot



NoBars

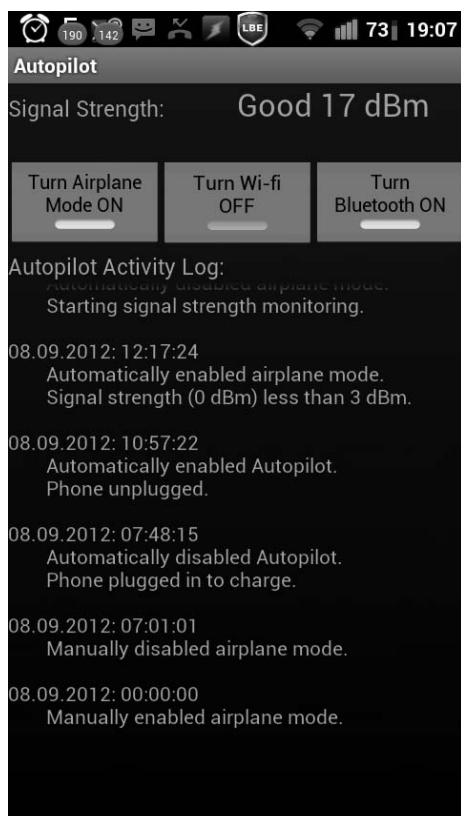


Bild A.7: *Autopilot* schaltet bei Signalverlust automatisch in den Flugzeugmodus – lässt auf Wunsch aber WLAN und Bluetooth an

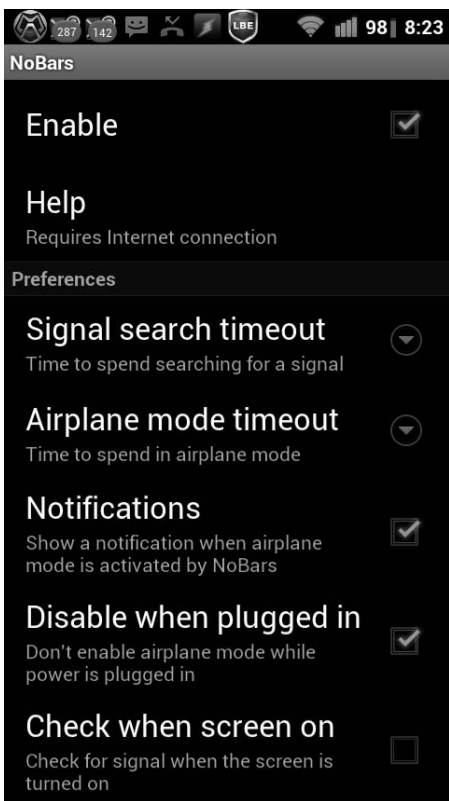


Bild A.8: Auch **NoBars** hilft, bei Signalverlust Strom zu sparen

Diese Apps (sowie die folgende *Tasker*-Lösung) habe ich jeweils unter vergleichbaren Bedingungen getestet. Ohne eine dieser Lösungen lag die Restladung meines Akkus nach ca. 11 Stunden bei etwa 60 Prozent. Sowohl *Autopilot* als auch *NoBars* schafften es, dies auf gut 70 Prozent zu verbessern. Meine *Tasker*-Lösung brachte es sogar auf fast 80 Prozent! Wie ist das zu schaffen?

Bei zu schwachem oder gänzlich abhanden gekommenem Signal (*Autopilot* erlaubt hier die Festlegung einer minimalen Signalstärke) versetzen die Apps den Androiden in den Flugzeugmodus. Nach einem festgelegten Zeitraum (bei *Autopilot* recht flexibel, bei *NoBars* hingegen nur grob einstellbar) wird der Flugzeugmodus wieder deaktiviert, sodass erneut die Signalstärke geprüft werden kann. Da im Flugzeugmodus das Radio-Modul deaktiviert ist, kann es auch keine (zusätzliche) Energie verbrauchen – so einfach ist das.

Wie sich das auf die Akku-Statistiken auswirkt, zeigt der Screenshot: Das *Telefonsignal* weist Löcher auf. Das sind die Zeiten, in denen sich das Gerät im Flugzeugmodus befand und demzufolge recht wenig Strom verbrauchte, was wiederum zu den längeren Akku-Laufzeiten führte.

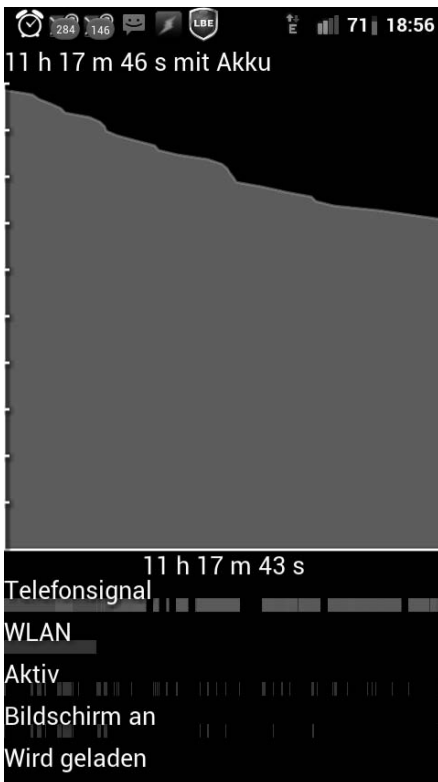


Bild A.9: Die Details zum Telefonsignal belegen die erfolgreiche Tätigkeit von **NoBars**

Welche der beiden Apps man nun einsetzen möchte, ist sicherlich eine Geschmacksfrage. Beide versahen ihren Dienst recht gut. *Autopilot* lässt sich umfangreicher konfigurieren, und bietet außerdem ein Protokoll; dafür schaltet es jedoch bei jeder Signalprüfung kurz den Bildschirm ein, was auf Dauer etwas nervt. *NoBars* gibt sich eher spartanisch, führt aber dennoch zu ebenso guten Ergebnissen.

Und dann wäre da schließlich noch die App, die diesem Kapitel den Namen gab. In vielen Android-Foren werden Fragen nach dem Universum-und-so-weiter nämlich nicht mit 42, sondern lediglich mit sechs Buchstaben beantwortet: T-A-S-K-E-R. Eine Sieben-Tage-Testversion von *Tasker* findet sich im Playstore, die Vollversion kostet ca. 5 Euro – und ist jeden Cent absolut Wert.

Wie im Screenshot zu sehen, habe ich mir also drei kleine Profile mit zugehörigen Tasks gebaut, die sich der Problematik *Mobilfunk-Standby* widmen sollen. Sie kommunizieren über eine gemeinsame Variable, die ich in meinem globalen *Init*-Profil initialisiere: In %SIGSTATE ist der aktuelle Zustand gespeichert. Dieser kann drei Werte annehmen: 0 (alles wunderbar), 1 (Signal relativ schwach) und 2 (Signal verschwunden).



Bild A.10: Tasker mit Profilen zum Stromsparen bei Signalverlust

Wenn %SIGSTATE kleiner als 1 ist, prüft *SigLowCheck* das Funksignal. Ist es unter einen eingestellten Wert (hier: 3) gefallen, werden die mobilen Daten deaktiviert (die würden jetzt nämlich auch zusätzliche Energie benötigen), und %SIGSTATE wird auf 1 gesetzt. Dieser Status bewirkt nun zweierlei: Zum einen wird *SigLowCheck* nun nicht weiter ausgeführt (Bedingung war ja: kleiner als 1), zum anderen schlägt nun sofort *SigReturnCheck* zu, welches nur bei einem Wert größer als 1 tätig wird.

SigReturnCheck setzt zunächst einen Timer und wird dann erst 5 Minuten später tätig. Es aktiviert die mobilen Daten wieder und deaktiviert den Flugzeugmodus. Dann setzt es erneut einen Timer und 15 Sekunden später die Variable %SIGSTATE auf 0 – womit es sich selbst deaktiviert und den anderen beiden Kandidaten den Weg frei macht.

Der Dritte im Bunde ist *SigLostCheck* und prüft (sofern %SIGSTATE kleiner ist als 2) das Funksignal. Fällt es unter den konfigurierten Schwellwert (2), wird in den Flugzeugmodus gewechselt und %SIGSTATE auf 2 gesetzt. Ein eventuell aktiviertes WLAN bleibt dabei auch aktiviert.

Um den Anwender auf dem Laufenden zu halten, blenden alle drei entsprechende Informationen im Nachrichtenbereich ein (siehe Bild). Der jeweils aktuelle Zustand steht dabei zuunterst, und das Neuauftreten eines Zustands (etwa der erneute Wechsel in den Flugzeugmodus) überschreibt den bereits vorhandenen Eintrag. War noch kein Eintrag vorhanden, macht sich auch der Vibrator kurz bemerkbar.

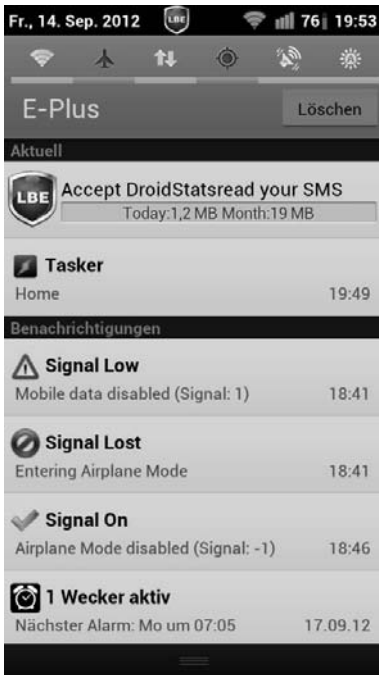


Bild A.11: Die **Tasker**-Profile berichten über ihre Tätigkeit in der Notification Area

Klingt doch ganz praktikabel. Und zum Nachbauen, hier die einzelnen Tasks sowie ihre zugehörigen Profile:

Task „InitVars“:

Variable → Variable Set: %SIGSTATE To 0

Task “SigLow”:

Net → Mobile Data: Off

Variable → Variable Set: %SIGSTATE To 1

Alert → Notify Vibrate:

Title: “Signal Low”

Text: „Mobile data disabled (Signal: %CELLSIG)“

Task “SigLost”:

Variable → Variable Set: %WLANSTATE To 0

Variable → Variable Set: %WLANSTATE To 1 IF %Wifi ~ on

Net → Airplane Mode: On

Net → Wifi: On IF %WLANSTATE ~ 1

Variable → Variable Set: %SIGSTATE To 2

Alert → Notify Vibrate:

Title: “Signal Lost”

Text: “Entering Airplane Mode”

Task „SigReturn“:

Task → Wait: 5 Minutes

Net → Airplane Mode: Off

Task → Wait: 15 Seconds (*dem Androiden Zeit geben, ein neues Signal zu finden!*)

Net → Mobile Data: On IF %ROAM ~ Off (*damit es nach dem Urlaub im Ausland keine böse Überraschung gibt: Nur wieder aktivieren, wenn nicht im Roaming!*)

Variable → Variable Set: %SIGSTATE To 0

Alert → Notify Vibrate:

Title: “Signal On”

Text: „Airplane Mode disabled (Signal: %CELLSIG)“

Profil SigLowCheck:

State → Variable → Variable Value:

Name: „%SIGSTATE“

Op „Math: Less Than“

Value „1“

State → Phone → Signal Strength: From 0 To 2

Task: SigLow

Profil SigLostCheck:

State → Variable → Variable Value:

Name: „%SIGSTATE“

Op „Math: Less Than“

Value „2“

State → Phone → Signal Strength: From 0 To 1

Task: SigLost

Profile SigReturnCheck:

State → Variable → Variable Value:

Name: „%SIGSTATE“

Op „Math: Greater Than“

Value „0“

Task: SigReturn

Profile Init:

Event → Tasker → Monitor Start

Task: InitVars

Wer mag, kann sich natürlich nach Belieben weiter austoben: Sound abspielen lassen, das Display zum Blinken bringen ... Aber die essentiellen Dinge zum Stomsparen sind alle bereits enthalten, einschließlich der Informationen zum aktuellen Status.

Anzumerken ist allerdings noch, dass es sich bei diesen Profilen lediglich um ein Grundgerüst handelt, welches noch einiger Anpassungen bedarf. So können sich beispielsweise

SigLowCheck und *SigLostCheck* ins Gehege kommen, wenn das Signal plötzlich wegfällt. Hier kann eine zusätzliche Bedingung in den beiden Profilen helfen:

State → Tasker → Task Running: „SigLost“, [x] Invert

im Profil *SigLowCheck*, und entsprechend umgekehrt in *SigLostCheck*. Ebenfalls möglich sind Kollisionen mit anderen Profilen, die sich mit dem Flugzeugmodus befassen. Auch wird das manuelle Aktivieren des Flugzeugmodus *SigLost* auslösen, was natürlich nicht erwünscht ist.

Dieses und weitere Dinge werden u. a. in einem Blog bei AndroidPIT behandelt.



<http://www.androidpit.de/tipps-zum-akku-fresser-mobil-funk-standby-teil-8>

A.5 Diebstahl-Schutz mit Tasker

Schrieb ich doch im Abschnitt 1.2 unter *Diebstahlschutz*, ein solcher ließe sich eventuell auch mit *Tasker* realisieren? In der Tat ist dies möglich. Eine Variante des „Device-Trackings“ (aka „Wo ist mein Android?“) stellt Kevin Purdy in einem Artikel auf Lifehacker.COM mit einer bebilderten Schritt-für-Schritt-Anweisung vor, zwar auf Englisch – aber dank der guten Bebilderung sollten schon geringfügige Sprachkenntnisse ausreichend sein, um dem How-To folgen zu können.



<http://lifehacker.com/5611003/build-a-find-my-iphone-clone-for-android>

Damit wäre die Lokalisierung eines abhanden gekommenen Androiden abgedeckt. Damit dies nicht in der Absicht eines „bösen Menschen“ geschieht (sondern allenfalls wir das Gerät „irgendwo liegen gelassen haben könnten“), hier noch ein kleiner Anreiz zur Umsetzung eines „Diebstahl-Alarms“. Selbiger soll losgehen, wenn ein Unbefugter sich unseres Androidens bemächtigt – nicht aber, wenn wir selbst ihn in die Hand nehmen. Dazu könnte wie folgt vorgegangen werden:

1. Profil 1: Bildschirm wurde entsperrt
 - Bedingung: Event → Display → Display unlocked
 - Task: Variable → Variable Set, U_UNLOCKING = 1
2. Profil 2: Alarm deaktivieren
 - Bedingung 1: Event → Hardware → Button: Camera
 - Bedingung 2: State → Variable Value U_UNLOCKING > 0
 - Task: Variable → Variable Set, U_UNLOCKING = 0
3. Profil 3: Alarm-Count-Down auslösen
 - Bedingung: State → Variable Value U_UNLOCKING > 0
 - Task: XXX

Bei „XXX“ ist natürlich die entsprechende Aktion einzusetzen. Beispielsweise mit einer While-Schleife zehn Sekunden warten, ob doch noch entschärft wird – und andernfalls anschließend ein entsprechendes MP3 abspielen, welches laut „DIEBE! ICH BIN EIN GEKLAUTES TELEFON!“ brüllt und dabei Polizeisirene, „Roten Alarm“ der Enterprise oder Ähnliches einblendet.

Wie ist das Ganze gedacht? Über eine Variable (U_UNLOCKING) schauen wir, ob überhaupt etwas passieren muss (ist sie ungleich 0?). Dazu wird sie bei Entsperrung des Bildschirms (ggf. durch andere Events wie „Gerät bewegt“ ersetzen) auf 1 gesetzt – dies erledigt „Profil 1“.

Wird nun beim/kurz nach dem Entsperren des Bildschirms der Kamera-Button gedrückt, gibt „Profil 2“ Entwarnung (setzt U_UNLOCKING=0; diese Aktion kann natürlich gegen einen beliebigen anderen Event ausgetauscht werden: etwa Umdrehen oder Schütteln des Androiden). Passiert dies nicht, kümmert sich „Profil 3“ um die entsprechende Alarm-Aktion.

Dies ist ein rein theoretischer Ansatz – sollte das jemand einmal umgesetzt haben, freue ich mich auf entsprechendes Feedback!

P.S.: Sollte das Gerät sich dennoch unerlaubt entfernt haben, so zeigt ein Video-Tutorial bei Youtube, wie sich auch die Ortung desselben mittels *Tasker* realisieren lässt.



<http://www.youtube.com/watch?v=DKV3Sv8Yvw8>

A.6 Secret Codes oder Magische Nummern

Klar kann man mit einem Telefon telefonieren. Dazu gibt man eine Ziffernfolge ein und drückt die Taste für „Wählen“. Was aber passiert, wenn man noch ein paar Sonderzeichen hinzufügt?

Disclaimer: Es kann sein, dass diese Codes nicht auf allen Geräten funktionieren. Wenn sie nicht im Handbuch des Gerätes aufgeführt sind, mag das durchaus seine Gründe haben: So kann der eine oder andere Punkt, unsachgemäß angewendet, u. U. Schäden verursachen. Ich übernehme keinerlei Garantien dafür, dass folgende Codes a) funktionieren, b) das tun, was da steht, oder c) „folgenfrei“ genutzt werden können. Insbesondere übernehme ich keinerlei Verantwortung für etwaige negative Folgen! Für etwaige positive Folgen stelle ich natürlich gern mein Bankkonto zur Verfügung ...

Es kann sein, dass nach Eingabe des einen oder anderen Codes nichts passiert. Es kann aber auch sein, dass dies nur so scheint (bei meinen Tests fand ich anschließend – am nächsten Tag – einige der „magischen Nummern“ in der „Verbraucherliste“ wieder). Es können hier durchaus Hintergrund-Dienste gestartet oder aber „versteckte Klassen/Menuis“ in Apps freigeschaltet werden ...

Code	Bedeutung
##0##*	Test des LCD-Displays
*#0011#	GSM-Infos
*#0228#	ausführliche Infos zum Barreriestatus
*##0283#**	Loopback-Test
**05*⟨PUK Code⟩*⟨neue PIN⟩* ⟨neue PIN zur Bestätigung⟩#	Entsperren des Telefons aus dem Notruf-Modus
*##0588#**	Test des Annäherungs-Sensors
*#06#	IMEI
*##0673#** *##0289#**	Einer der beiden Codes führt zu einem Audio-Test
*#0782#	RTC (Real-Time-Clock) auslesen und anzeigen
*##0842#**	Test für Vibrator (oh ja!) und Hintergrund-Beleuchtung
*##1111#**	FTA Software Version
*##1234#**	Firmware-Info
*135#	Eigene Rufnummer anzeigen
*##1472365#**	ein kurzer GPS-Test (und Einstellungen)
*##1575#**	ein weiterer GPS-Test
*##197328640#**	Service-Menü mit verschiedenen Test-Möglichkeiten
*#21#	Status der Anrufweiterleitungen überprüfen
*##2222#**	FTA Hardware Version
*#2263#	Bandnutzung
*##232331#**	BlueTooth-Test
*##232337#**	MAC-Adresse des BlueTooth-Interfaces
*##232338#**	MAC-Adresse des WLAN-Interfaces anzeigen
*##232339#** *##526#** *##528#**	Einer dieser Codes führt zu den WLAN-Tests...

Code	Bedeutung
##2432546## (*##CHECKIN##*)	Nach <i>OTA</i> -Updates suchen
##2663##	Touch-Screen Version anzeigen
##2664##	Touch-Screen Test
*##273283*255*663282*##*	Angeblich für eine schnelle Sicherung der Medien-Dateien (Fotos, Videos..) gut. Von wo und nach wo? Habe ich nicht probiert ...
*2767*3855#	Factory Format (<i>Wipe</i>). Vorsicht damit!!!
#31#<Rufnummer>	Mit unterdrückter Rufnummer anrufen
##3264##	RAM Test / RAM-Version anzeigen
##3424##	HTC Function Test
##34971539##	Kamera-Menü mit folgenden Punkten: Update mit Firmware aus Bild (keinesfalls! Sonst futsch!); Update mit Firmware von SD-Karte; Versions-Info; Update-Counter
*43# / #43# / *#43#	Anklopfen aktivieren / deaktivieren / Status abfragen
##44336##	Herstellungszeitpunkt und Laufende Nummer
##4636## (*##INFO##*)	Öffnet ein Menü, aus dem sich wählen lässt: Telefon-Infos, Akku-Infos, Akku-History, Verbrauchsstatistiken. Der Umfang kann je nach Android-Version unterschiedlich ausfallen.
#4646#	Feldtest (Details zu Akkustand + Funknetz, Wechsel UMTS/GSM)
*##4986*2650468##*	Diverse Hardware-Infos
##564##	QXDM (Qualcomm eXtensible Diagnostic Monitor) Logging FrontEnd
##7262626##	Ein Bett im Kornfeld ... äh, Feld-Test
##7269##	Standard Device-Logging (Device [logcat?], AT-Befehle, Kernel [dmesg?] -- HTC?)

Code	Bedeutung
*#7465625#	Netz- und Subnetzsperrung, Simlock, Service Provider und Corporate Lock (Galaxy-S?)
#7594#	Verhalten des Einschalt-Knopfes ändern (z. B. direktes Abschalten ohne Menü)
#7780#	Zurücksetzen auf Werkseinstellungen
#8255#	GoogleTalk Service Überwachung
#8350#	Logging der Anrufe deaktivieren
#8351#	Logging der Anrufe aktivieren
*#9090#	Service-Modus UART/USB
#9696#	FTP Test
*N# (TCom: *T#)	Wird eine SMS mit dieser Zeichenfolge begonnen, erfolgt eine SMS Empfangsbestätigung

A.7 Leistungsaufnahme verschiedener Komponenten

Heise hat für seinen Artikel *Energiesparplan* ein Motorola Milestone angepasst und ausführlich getestet, was welche Komponente verbraucht und wie man das einschränken kann (das war jetzt eine klare Empfehlung, den Artikel zu lesen!). Die Daten davon werden einerseits ein „war ja klar“, aber bei einigen Daten auch ein „oh, das hätte ich jetzt nicht gedacht“ hervorrufen. Passende Angaben zum Galaxy S3 hat die c't in ihrer Ausgabe vom August 2012 gesammelt – und dabei den Test gleich noch ein wenig ausgeweitet.

Anmerkungen zum Galaxy S3 (*): Der Energieverbrauch des Displays hängt auch stark von den dargestellten Inhalten ab, was auf das verwendete AMOLED-Display zurückzuführen ist: Bei vollständig schwarzem Display entspricht der Verbrauch auf allen Stufen nicht mehr als dem Minimum.



http://www.heise.de/artikel-archiv/ct/2012/17/124_kiosk



<http://www.heise.de/mobil/artikel/Tipps-und-Tools-fuer-eine-bessere-Akkulaufzeit-unter-Android-1145579.html>

Weiterhin sollte man beim Vergleich der Werte auch die unterschiedliche Hardware-Ausstattung im Hinterkopf behalten: So werkelt beispielsweise im Galaxy S3 ein mit 1,4 GHz getakteter Quad-Core-Prozessor, und zur Anzeige dient ein 4,8-Zoll-Display – im Milestone waren es noch eine Single-Core-CPU mit 550 MHz und ein 3,7-Zoll-Display.

Betriebszustand	zusätzliche Leistungsaufnahme	
	Motorola Milestone	Samsung Galaxy S3
Videoaufnahme ¹	1557 mW	1683 mW
UMTS Upload	1410 mW	1033 mW
UMTS Download	1349 mW	1074 mW
EGDE Upload	1179 mW	
WLAN Download	1158 mW	549 mW
Video abspielen (fullscreen) ¹	1135 mW	597 mW
UMTS-Telefonat	983 mW	637 mW
Kamera ¹	934 mW	1460 mW
EGDE Download	853 mW	
Bluetooth empfangen	751 mW	487 mW
Display (höchste Stufe)	730 mW	1568 mW*
GPS Suche	550 mW	263 mW
GSM-Telefonat	511 mW	297 mW
Bluetooth senden	487 mW	454 mW
WLAN Upload	479 mW	488 mW
Display (niedrigste Stufe)	310 mW	567 mW
WLAN Tether ²		372 mW
MP3 abspielen über Bluetooth		296 mW
MP3 abspielen	160 mW	153 mW
UMTS Standby	18,3 mW	13,8 mW
GSM/EDGE Standby	11,6 mW	9,5 mW
WLAN Standby 2,4 GHz	7,8 mW	9,3 mW
WLAN Standby 5 GHz	N/A	14,6 mW
NFC Standby	N/A	4 mW
Bluetooth Standby	2,8 mW	1,8 mW
GPS Standby	0,4 mW	0,7 mW
WLAN Tether Download ³		1254 mW

¹ Leistungsaufnahme des Displays bereits abgezogen, ² Tethering aktiv, 1 Benutzer, ³ Download vom Notebook per WLAN-Tether

Für die Gesamt-Leistungsaufnahme muss natürlich noch die Grundlast hinzugerechnet werden (was das Gerät verbraucht, wenn alles in der Tabelle benannte abgeschaltet ist; also „Flugmodus“). Das wären ganze fette 6,4 mW. Wird das Gerät also des Nachts in diesen Modus versetzt, spart das bereits enorm:

Betriebszustand	zusätzliche Leistungsaufnahme	
	Motorola Milestone	Samsung Galaxy S3
Flugmodus	6,4 mW	6,4 mW
GSM Bereitschaft	18 mW	9,5 mW
GSM Bereitschaft + WLAN Standby	25,8 mW	18,8 mW
GSM Bereitschaft + WLAN Standby + Bluetooth Standby	28,6 mW	20,6 mW
UMTS Bereitschaft	24,7 mW	10,9 mW
UMTS Bereitschaft + mobile Daten aktiv		13,8 mW
UMTS Bereitschaft + WLAN Standby	32,5 mW	20,2 mW
UMTS Bereitschaft + WLAN Standby + Bluetooth Standby	35,3 mW	22,0 mW

Die Werte sind natürlich alle spezifisch für o.g. Motorola Milestone bzw. das Samsung Galaxy S3 und können auf anderen Geräten abweichen. Die Größenordnungen sollten aber zumindest ähnlich sein.

Nochmal gesagt: Selbst wenn WLAN etc. alle aus sind und nur Telefonate (und SMS) noch durchkommen (den Datenverkehr also mal ganz außen vorgelassen), reduziert sich der Verbrauch im Flugmodus auf ein Drittel (GSM) oder gar ein Viertel (UMTS). Einmal sechs Stunden angenommen (von 0 Uhr bis 6 Uhr), hält der Akku damit (theoretisch) für bis zu gut zwei Stunden länger. Natürlich wieder nur, wenn man dann anschließend auch nichts damit macht – also wieder so ein „Laborwert“. Trotzdem kann man sich leicht ausrechnen: Sechs Stunden Flugmodus (statt GSM Bereitschaft) schaffen Raum für zusätzliche ca. acht Minuten GSM-Telefonat.

Symbole

1Tap Cleaner 250

3G Watchdog 200

<package_name>-Verzeichnis 114

A

Access Point Name 295

ADB 128, 294

ADB-Backup 283

ADB Browser 177

ADB FileExplorer 177

AdBlock 208, 210

AD Blocker & Net Toggle 209

adb shell

 bugreport 132

 dmesg 128

 dumpstate 130

 dumpsys 130

 logcat 129

Ad-Detector 78

AdFree Android 208

Administration 191

Administrator 304

Advanced Tools 170

Advanced Users Toolbox 170

AES 57, 294

AirPush 77

AirPush Detector 78

Akku 150

 kalibrieren 262

 laden / entladen 262

 Temperatur 262

Akku-Laufzeit 246

Akkulaufzeiten 256

Akku-Pflege 261

Akkuverbrauch 288, 319, 329

Akkuverbrauchs-Informationen 150

Alarms-Verzeichnis 114

Alarmton 114

aLogcat 126

AmonRa 178

AndFTP 43

Android Audio Profile 158

Android Backup Extractor 284

Android Debug Bridge 294

Android Hotspot Login 222

Android Location Cache Viewer 68

Android Open Source Project 182, 294

Android Package 294

Android-SDK 294

Android Settings 285

Android System Info 123

AndSMB 42

Anrufeinstellungen 139

Anti-Malware 74

Anti-Theft-Apps 81

Anti-Viren-Apps 71

Anti-Virus 74

Anti-Virus Free 75

Anwendungen 143

Anwendungs-Cache 110

Anwendungs-Daten 110

AOKP 186

AOSP 132, 182, 294

AOSP-ROM 183

APG 51

API 294

APK-Datei 294

APN 138, 295

APN Backup & Restore 27

APNdroid 201

App 295

App2SD 110, 286

App2SD+ 111

AppBrain Ad-Detector 79

App-Daten 87

AppExtractor 16

Application Programmers Interface 294

Application Protection 60

AppMonster 21

App Quarantine 248

Apps

 am automatischen Starten hindern 251

 auf SD-Karte 286

 auslagern 271

 deinstallieren 247

- Passwort-Sicherung 58
- Quelle 70
- Sicherheit 84
- sichern 21
- Sicherung 285
- updaten 287
- Zertifikat 91
- App Schutz Einrichtung 59
- App-Sicherheit 84
- AppSync 24
- appWatchdog 89
- ASTRO Datei-Manager 165
- AutoKiller Memory Optimizer 273
- Automatisierung 156
- Auto Memory Manager 273
- Autopilot 319
- Autorun Manager 252
- Autostarts 253
- Auto WiFi Toggle 215

B

- Backup
 - in die Cloud 29
 - Komplett-Backups 16
 - Kontakte 25, 31
 - lokale Backups 12
 - Nandroid Backup 15
 - SMS 25, 31
- Backup Bookmarks 28
- Barnacle Wifi Tether 219
- Baseband 295
- Battery Calibration 263
- Battery Calibrator 263
- Battery Saver 216, 268
- Benachrichtigungston 114
- BetterBatteryStats 136
- Bewertungen 70
- Bilder 114
- Blade Buddy 154
- Bloatware 86, 183, 248, 295
- Bluetooth 65, 188
- Bluetooth Firewall 65
- Bookmarks 28

- Bookmark Sort & Backup 28
- Bootloader 101, 295
- boot-Partition 111
- Boot-Partition
 - alternative 111
- Boot-Prozess 99
- Boot-ROM-Code 101
- BoxCryptor 40
- Brain 2.0 69
- Brick 296
- Browser-Lesezeichen 285
- bugreport 132
- Bug Reporter 127

C

- Cache
 - bereinigen 249
- Caesar's Cipher 48
- CalDav 296
- Call Logs Backup & Restore 27
- cgroup 105
- cgroups 106
- Child App Protector 58
- CifsManager 202
- ClockworkMod Recovery 15, 178
- Cloud 29, 37
- cnlab SpeedTest 199
- Comma Separated Values 296
- ConnectBot 206
- CPU-Tuner 156, 276
- CPU übertakten 276
- CPU untertakten 264
- Crypt Haze 50
- CSV 296
- Custom Recovery 178
- Custom-ROM 178, 184, 296
- CyanogenMod 184, 185

D

- Dalvik 297
- Dalvik-Cache 110
- Dalvik-VM 102, 297
- Data Encryption Standard 297

data-Verzeichnis 111
 Datei-Manager 164, 169
 Datei-Server 234
 Dateisysteme 102
 cgroups 106
 devpts 105
 eingebundene 110
 EXT 108
 FAT32 109
 proc 106
 rootfs 105
 Sysfs 105
 tmpfs 108
 VFAT 109
 virtuelle 105
 YAFFS2 109
 Datenschutz 144
 Datenstrukturen 110
 Datensynchronisation 189
 Datenverbrauch 200
 Datenverwaltung 172
 Datum 149
 DavDrive 237
 Dazzle 120, 259
 DCD CloudSync 41
 dcim-Verzeichnis 114
 Debuggen 297
 DES 294, 297
 devices 110
 devpts 105
 DHCP 190, 297
 Diebstahlschutz 80, 325
 Dienste 230
 Deaktivierung ungenutzter 257
 DiskUsage 292
 Display 140, 329
 Display-Einstellungen 258
 dmesg 128
 DNS 298
 Domain Name System 298
 Downloads 114
 Download-Verzeichnis 114
 Drahtlos und Netzwerke 138

DrainGuard 256
 Droid Crypt 57
 Droid Explorer 19, 283
 DroidDrive 30
 DroidWall 65
 Dropbox 38
 Dropbox-App 38
 Dropbox Sync for Tasker Locale 39
 DropSnap 40
 DropSpace 40
 DropSpace Plugin for Tasker 40
 Dr.Web Anti-virus 74
 DSP Equalizer 186
 dumpstate 130
 dumphsys 130
 Dynamic Host Configuration Protocol 297

E

EasyProfiles 159
 EasyTether 232
 Eds 56
 eFile 169
 Eingabehilfen 148
 Eingebundene Dateisysteme 110
 Einschalten 101
 Einstellungen
 ausgewählte 151
 häufig genutzte 151
 versteckte 153
 zusätzliche 153
 Elixier 2 116, 122
 EmailProvider.db 87
 eMMC 110, 298
 Emulierte MultiMediaCard 298
 Encrypt It 50
 Enigma 49
 ES Datei Explorer 164
 Eventbasiertes Schalten 159
 EXT 102, 108
 Extended File System 102, 108
 eXtensible Markup Language 309
 Externer Speicher 114

F

Facebook 35
Fastboot 298
Fast Uninstaller 248
FAT32 109
File Expert 238
File Transfer Protocol 298
Filme 114
Firewalls 65
Flashen 298
FolderSync 45
foremost 283
Fotos 114
FTP 234, 298
FTP-Server 43, 236
FTPSyncX 44
Funambol Sync 36

G

Geräte-Dateien 110
Gespeicherte Daten 84
Ghost Commander 167
Gibberbot 205
Global Positioning System 299
G-MoN für Android 229
GMV 69
GNU Privacy Guard 298
Google Backup 285
Google Permissions 302, 309
Gordian Secret Code Tool 48
GotYa! Face trap 82
GPG 298
GPS 141, 188, 258, 299
Green Power 267
Grundlast 331
Gschockt 31

H

Hardreset 299
Hersteller-Apps 86
Hintergrunddaten 259
Hotspot 217, 222

HotSpot Login 223
HTTP 299
HTTP Proxy-Settings 204
HTTPS 299
HyperText Transport Protocol 299
Secure 299

I

iCal 299
iCalendar 299
iCal Import/Export 27
ICSSync 35
IMEI 299
Incognito Mode 186
Init-Prozess 101
International Mobile Station Equipment
Identity 299
Interner Speicher 270
Internet-Verbindung
Firewall 65
IntraNet 300

J

JuiceDefender 266

K

Kalender 27, 35
Kalenderdaten 182
Kaspersky Mobile Security 72
Kernel 111, 300
Keyhole Markup Language 300
Klingelton 114
KML 300
Komplett-Backups 16
Komplett Sicherungen 13, 30
Komponenten 329
Konfiguration 137
Bordmittel 137
Konfigurations-Dateien 110
Kontakte 25, 31, 35
Konten 142
kWS 241

L

Laufwerke 202
LBE Privacy Guard 64, 201
LCDDensity 156
Leistungsaufnahme 329, 331
Lesezeichen 28
Lesezeichen-Manager 169
LiIo 262
Link2SD 271
Linux-Kernel 101
LiPo 262
Lithium-Ionen-Akkus 262
Lithium-Polymer-Akkus 262
Live-Wallpaper 261
Llama 158
Locale 160
Location Cache 47, 67, 137
Location Profile 158
Lockscreen-Gesten 186
logcat 129
Log Collector 127
Logdateien 125, 132
Lokale Backups 12
Lookout Security Antivirus 71
LUKS Manager 55

M

MAC-Adresse 300
Magische Nummern 326
main.db 88
Malware 47, 69
Media-Access-Control-Adresse 300
Media Show 243
Medien 293
Medien-Scanner 293
Medien-Server 243
Mini Info 117
mIQ 30
MMS 182
Mobile Backup II 26
Mobiler Hotspot 217
Mobilfunk-Standby 288, 290, 319

Mobilnetze 138
MobiPerf 197
Monitoring 133
Mount Manager 203
Mount Points 110
Movies-Verzeichnis 114
MultiMedia-Metadaten 182
Music-Verzeichnis 114
Musik 114
MyAntiVirus Pro 76
MyBackup Pro 19
MyPhoneExplorer 172
MySettings 120

N

NAND-Flash 103, 180, 300
Nandroid Backup 15, 180, 285, 300
NAS 301
NeoRouter 213
NetQin Security & Anti-virus 73
Net Status 198
Network Attached Storage 301
Network Booster 290
Network File System 301
Network Info II 193
NetworkLocationLocator 137
Netzwerk
 Diagnose 193
 Geschwindigkeit 198
 Server können nicht erreicht werden 194
Netzwerk-Konfiguration 187
Netzwerk-Verbindung 193
NFS 301
NoBars 319
Norton Mobile Security 72
No Signal Alert 289
Notification Area 301
Notifications-Verzeichnis 114
Nutzerwörterbuch 147

O
OnTheFly Backup 22
OOM-Killer 255, 301

OpenPGP Manager 52
OpenSignalMaps 289
OpenVPN 186, 212
Orbot 205
Orkut Contact Sync 34
Ortsbasiertes Schalten 159
Ortsbestimmung 141
Orweb\
 Proxy+Privacy Browser 205
OS Monitor 123
OTA 301
Out Of Memory 301
Over The Air Update 301

P

Partition 110, 111, 302
Passman 55
Passwort-Safes 53
PAW Server 175
PC
 zur Android-Verwaltung 172
PdaNet 219
Peer-to-Peer 302
Permission 61, 70, 302
 überprüfen 62
 überwachen 63
 Umgang mit 61
Phone-Goggles 186
Phone Profiles 159
Pictures-Verzeichnis 114
PIN'r 53
Pi.Soft Backup 25
Pleex Mobile Backup 31
Pocket Enigma Machine 49
Podcast 114
Podcasts-Verzeichnis 114
Port-Forwarding 235
Privacy Blocker 64
proc 106
procf 103
Profile 323
Profil-Eigenschaften 159
Proxoid 232

Proxy 204, 302
ProxyDroid 155, 205
Prozess-Informationen 110
Push-Notifications 77

Q

qNetInfo 191
QtADB 177
Quick App Manager 249
Quick Cache Cleaner 250
Quick Settings 151
QuickSSHd 237

R

Radio Unit Update 304
RAM 303
 bereinigen 273
RAM-Disk 111
Random Access Memory 303
Read Only Memory 303
Recovery 178
Recovery-Menü 303
Recovery-Partition 111
Reguläre Ausdrücke 303
Reiser File System 103
reiserfs 103
Remote-Laufwerke 202
Remote Web Desktop 146, 174
Rescan SD Card! 293
Reverse Tether 220
Ringtones-Verzeichnis 114
RL Permissions 62
Roaming 188
ROM 303
ROM Manager 179, 185
ROM Upgrade Utility 304
root 93, 304
root-Dateisystem 105
Root Explorer 167
rootfs 105
root-Zugang 93
 Risiken 95
 Vorteile 94

RSA 304
Rücksetzen auf Werkseinstellungen 299
Rundum-Sorglos-Pakete 71
RUU 304

S

Safety 12
Salt 305
Samba 236
Samba Filesharing 236
Samba-Server 42
Sandisk Memory Zone 292
Scalpel 283
Schnellumschalter 119, 258
sd-ext 285
sd-ext-Partition 111
SDK 305
SD-Karte 114, 145, 286
 externe 110
 interne 110
 Klasse 287
SD Maid 270
Secret Codes 326
Secret Phone Settings 155
SecretVault 56
Secure Shell 306
Security 47
Sense Analog Clock Widget 4x2 118
ServDroid.web 242
Server Message Block 236, 305
Server-Side Includes 306
Servers Ultimate 234
Service Set Identifier 306
Session Initiation Protocol 305
SetCPU 156, 264
Set DNS 155
Shake-Uninstall 248
Sichere Übertragung 204
Sicherheit 12
 Datenübertragung 204
Sicherheits-Manager 169
SIP 305
SmartSync 156
SMB 305
SMS 25, 182
SMS Backup + 31
SMS Backup & Restore 26
Sniffer 305
Spare Parts Plus 153
Speed 246, 272
Speedtest.net Mobile 198
Speicher
 aufräumen 270
Speicherplatz 291
Sprache 146
Spracheingabe/-ausgabe 147
Sprite Backup 20
SQLite-Datenbank 88, 182
SQLiteMan 182
SSH 128, 237, 306
SSH Tunnel 204
SSI 306
SSID 306
Standort und Sicherheit 141
Startup Auditor 254
Statusbereich 301
Statusleiste 301
Stock ROM 182
SU File Manager & Terminal 168
SuperOneClick 95
SuperPower 268
Super-User 93, 304
Swap-Datei 275
Swapper 275
Swap-Space 275
Sweet Home 42
SWifis 227
SviFTP 234
Symlink 306
Synchronisation 33, 35, 143
 Cloud 45
 Kalender 35
 Kontakte 35
Synchronisierung 259
sysfs 105
Sysfs 105

System-Dateien
 vorinstallierte 110
System-Daten 85
Systemeinstellungen
 Anrufeinstellungen 139
 Anwendungen 143
 Datenschutz 144
 Datum und Uhrzeit 149
 Display 140
 Drahtlos & Netzwerke 188
 Drahtlos und Netzwerke 138
 Eingabehilfen 148
 Konten 142
 SD-Karte 145
 Sprache 146
 Spracheingabe/-ausgabe 147
 Standort und Sicherheit 141
 Synchronisierung 143
 Tastatur 146
 Telefoninfo 149
 Telefonspeicher 145
 Tethering 233
 Tethering & mobiler Hotspot 217
 Töne 139
System-Informationen 110
Systeminfo-Widgets 116
System Logs 125
SystemPanel 133
System-Server 102
Systemspeicher 303
System Tuner 135
System-Verzeichnis 111

T

Tape Archive 306
TAR 306
Tasker 156, 161, 214, 319, 321, 325
Tasker-Profile 323
Task-Killer 255
Task-Manager 169
Tastatur 146
Telefoninfo 149
Telefonspeicher 145

TestDisk 283
Tethering 217, 231, 306
The Onion Router 307
Thief Alarm 80
Timeriffic 157
Titanium Backup 13, 248
tmpfs 103, 108
Töne 139
Toneinstellungen 140
Toolboxen 169
TOR 307
TotalCare – Remote Security 83
Total Commander 166
Traceroute 195
Traces 307
Tracker 307
TrueCrypt 55
Tuning 245
 Geschwindigkeit 272
Tuning-Maßnahmen 245, 247
Tunnel 204, 206, 307
Txxtract MM & SMS Backup 27

U

Übertragene Daten 89
Uhrzeit 149
unyaffs 181
Update.Zip 307
USB-Stick 230
USB-Tethering 231

V

Vendor-ROM 183
Verschlüsselung 47
 Dateien 55
 Texte 47
 Verzeichnisse 55
Verzeichnisse 111
vfat 103
VFAT 109
Videos 114
Viren 47, 69
Virtual File Allocation Table 103

Virtual Network Computing 308
Virtuelle Dateisysteme 105
Virtuelles Privates Netzwerk 308
Visual Traceroute 196
Visual Tracert 197
VNC 308
VPN 211, 308
VPNC Widget 212
VPN-Einstellungen 138
VPN Show 211

W

War-Driving 228
WatchDroid 82
Web-based Distributed Authoring and Versioning 308
Web-Bug 308
WebDAV 236, 308
Web-Server 239
WeFi 225
Werbung 77
WhatsApp Messenger 89
Wheres My Droid 81
Widgets 116, 260
Widgetoid 2 121
WiFi Advanced Config Editor 155, 190
WiFi Auto On 215
WiFi File Transfer 239
WiFi Location Toggle 214
WiFi Manager 226
Wifi Static 190
WiFi Web Login 225

Wigle Wifi Wardriving 229
Wipe 309
Wireless File Transfer 240
Wireless Tether for Root Users 218
WLAN 138, 211, 258, 331
 automatische Aktivierung 213
WLAN-Accesspoints 85
WLAN-Finder 222
WLAN-Hotspot 217
WLAN-Konfiguration 189
wpa_supplicant.conf 85
Wuala 37

X

XING 34
XING-App 34
XING Sync 34
XML 309

Y

YAFFS 103
YAFFS2 109
Yet Another Flash File System 103

Z

Zeitbasiertes Schalten 159
Zeitschaltuhren 157
Zertifikat 91
Zugangspunkte 138
Zugriffsrechte 47, 61, 302
Zygote 102

Andreas Itzchak Rehberg



Das inoffizielle

Android System-Handbuch

Dieses Buch enthält tiefgehendes Insider-Wissen zu Android, dem beliebtesten Mobile-Betriebssystem weltweit. Erfahren Sie, mit welchen Tools Sie Ihr Android-Gerät schneller und sicherer machen, wie Sie an die System-Informationen herankommen und wie Sie eine optimale Konfiguration erreichen.

Mehr Platz, mehr Geschwindigkeit und höhere Sicherheit für Ihren Androiden!

Tuning

Passen Sie den Androiden Ihren Bedürfnissen an und machen Sie ihn schneller. Schaffen Sie mehr Platz im internen Speicher und verlängern Sie die Laufzeit Ihres Akkus durch konsequentes Umsetzen der Tipps und Empfehlungen, die Sie hier finden.

Systemkonfiguration

Lernen Sie die Datenstrukturen und Dateisysteme kennen, die auf Ihrem Androiden angelegt sind, und rufen Sie wichtige System-Infos mit den Bordmitteln von Android oder zusätzlichen Tools ab. Auch die Konfiguration von Netzwerken und die Automatisierung von Aufgaben wird ausführlich beschrieben.

Sicherheit

Erfahren Sie hier, welche Anti-Viren-Apps Sinn machen, wie Sie lokale Backups oder Backups in der Cloud erstellen und was die Google Permissions bedeuten, die Apps bei Ihrer Installation von Ihnen verlangen.

Aus dem Inhalt:

- Lokale Backups
- Backup in die Cloud
- Synchronisation
- Die Google Permissions und was sie bedeuten
- Anti-Virus und Anti-Malware
- Der Super-User „root“
- Dateisysteme und Datenstrukturen
- System-Infos: Widgets, Schnellumschalter und Monitoring
- Automatisierung: zeit-, orts- und eventbasiertes Schalten
- Tasker
- Systemkonfiguration
- Dateimanager
- Android vom PC aus verwalten
- Custom Recovery und Custom-ROMs
- Netzwerkkonfiguration
- WLAN
- VPN
- Tethering
- Tuning: Need for Speed
- Längere Akkulaufzeiten
- Vorinstallierte Apps entfernen
- Mehr Platz im internen Speicher
- Begriffserklärungen rund um Android

Über den Autor:

Andreas Itzchak Rehberg ist Informatiker und freiberuflicher Oracle-Datenbank-Administrator. Als begeisterter Android-User ist er seit 2010 Mitglied bei AndroidPIT, der größten Android-Community in Deutschland, und zählt dort zu den Top Ten der Aktiven.



Besuchen Sie unsere Website
www.franzis.de



30,- EUR [D]
ISBN 978-3-645-60215-0

FRANZIS