FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensik mobiler Endgeräte

Stefan Maus
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Inhaltsverzeichnis

Was sind mobile Endgeräte?

- Geräte, die durch ihre Größe und Form mobil nutzbar sind
- Sie dienen der Informations- und Kommunikationstechnik
- Zeichnen sich aus durch
  - Ortunabhängige Nutzung von PIM Daten
  - Unterstützung von GSM, UMTS
  - WIFI
  - GPS
- Dazu gehören Smartphones, Handys, PDAs, Navigationsgeräte und Note- bzw. Netbooks

Betriebssysteme

Smartphone Betriebssysteme:

- Apple iOS 4.3.2
- Google Android Froyo 2.2 & Gingerbread 2.3

- Windows Phone 7
- RIM Blackberry OS
- Nokia Symbian

Apple iOS 4

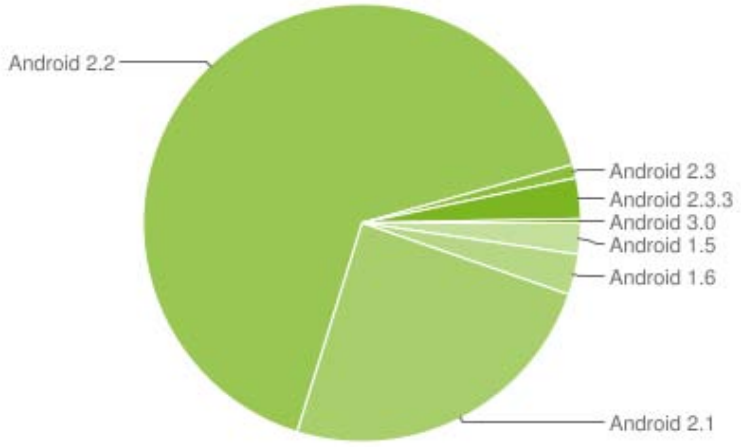
- Basiert auf Mac OS X
- Angepasst auf die ARM-Prozessoren
- Dateisystem HFSX
- Benötigt iTunes zum Synchronisieren und zum Datenabgleich
- Einsatz auf iPhone, iPad und Apple TV
- 16.2 Millionen iPhones im Q4 2010 verkauft

Google Android

- Entwickelt von der Open Handset Alliance
- Smartphones, Netbooks und Tablets
- Täglich werden 350.000 Android-Geräte aktiviert
- Ca. 33.3 Millionen Geräte verkauft in Q4 2010

Google Android

Mehrzahl der Besitzer nutzen Froyo 2.2



Platform	API Level	Distribution
Android 1.5	3	2.3%
Android 1.6	4	3.0%
Android 2.1	7	24.5%
Android 2.2	8	65.9%
Android 2.3	9	1.0%
Android 2.3.3	10	3.0%
Android 3.0	11	0.3%

Quelle: http://developer.android.com/resources/dashboard/platform-versions.html

Google Android - Aufbau

- Basiert auf Linux Kernel 2.6
- Jede Anwendung läuft
  - als eigener Prozess
  - in eigener virtuellen Maschine (Dalvik VM)
  - mit eigener User-ID
- Trotzdem Zugriff auf Daten anderer Programme, wenn freigegeben
- Datenspeicherung in XML-Dateien und SQlite Datenbanken

Verbreitung & Marktanteil

Marktanteil in Deutschland

OS	Marktanteil März 2011 (%)	Marktanteil Januar 2011 (%)	Impressions März 2011 (Mio.)	Impressions Januar 2011	Veränderung %
Android	49,7	24,6	257,8	115,6	123,1
iPhone OS	30,1	39,1	156,0	183,7	-15,1
Symbian OS	6,9	13	36,0	61,2	-41,2
RIM OS	2,1	1,9	10,7	9,1	16,9
Nokia OS	1,8	2,5	9,5	11,9	-20,0
andere	9,4	18,8	48,7	88,8	-45,2

InMob Mobile Insights März 2011

Forensische Analyse

Analysemöglichkeiten:

- Softwarelösung
  - Paraben Device Seizure
  - Katana Lantern 2.0
- Software/Hardware Kombination
  - Cellebrite UFED Physical Pro
- Manuell

Android Analyse

Analyse eines HTC Desire 2.2 mit CustomRom

- Root-Zugriff ?
- Auswertung über die Android Debug Bridge (adb)
- Nandroid Backup

Root-Zugriff

- Root-Zugriff wird benötigt, um direkt auf Anwendungsdaten zuzugreifen
- Ansonsten nur über zu installierende Applikation möglich => API Provider
- Vollzugriff kann über eine Lücke in der adb erlangt werden => rageagainstthecage Exploit

⇒ Zugriff auf alle forensisch relevanten Daten

⇒ /data/data/<<applikation>>

Android Debug Bridge

Verbindung über USB mit Android Shell möglich

`=> adb [-d|-e|-s <serialNumber>] <command>`

- Datentransfer
  - `push || pull <local> <remote>`
- Installation
  - `install <path_to_apk>`
- Auslesen der Logdateien
  - `logcat`
- Auslesen der Systemeinstellungen
  - `getprop > getprop.forensic`

Geolocation Daten

- Das Android speichert kontinuierlich Geo-Daten
  - `/data/data/com.google.android.location/cache.*`
- cache.cell
  - Speichert 50 Einträge

key	accuracy	conf.	latitude	longitude	time
262:7:31627:21480016	1977	75	50.914369	6.356387	04/19/11 22:24:31 +0200

- cache.wifi
  - Speichert 250 Einträge

key	accuracy	conf.	latitude	longitude	time
bc:05:43:2e:8e:d1	86	92	50.817368	6.263719	04/17/11 20:32:30 +0200
00:13:f7:a4:11:19	75	87	50.817479	6.263579	04/17/11 20:32:30 +0200
00:24:fe:40:2d:3a	80	92	50.817369	6.264440	04/17/11 20:32:30 +0200

Geolocation Daten

Die Speicherung erfolgt in Binärdateien

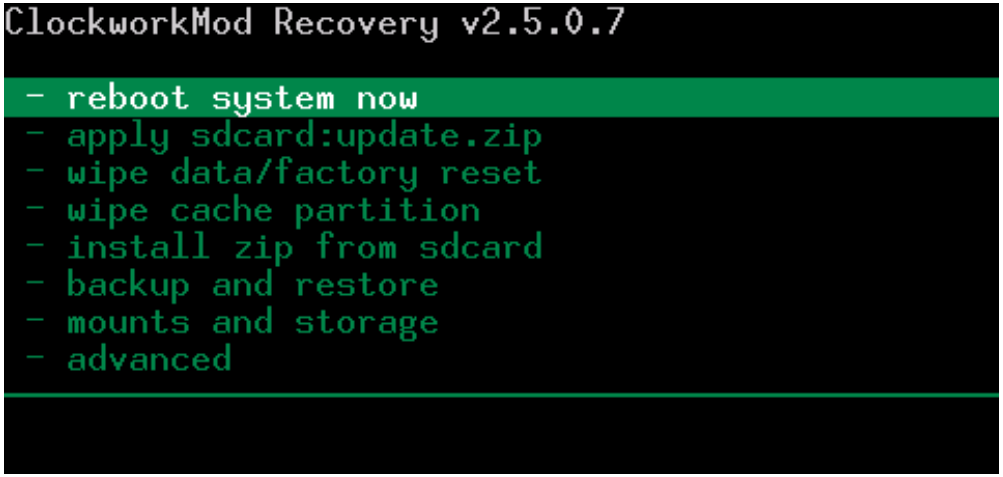
Dateianfang: 2 Byte DB-Version + 2 Byte DB-Entries

- Keylength 2 Byte (Int16)
- Key Byte*Keylength (String||Char)
- accuracy 2 Byte (Int16)
- confidence 2 Byte(Int16)
- latitude 8 Byte (double)
- longitude 8 Byte (double)
- timestamp (int64||long)

05C	F8	C1	00	12	32	36	32	3A	31	3A	38	32	32	34	3A	32	35	38	35	31	38	34	00
073	00	05	05	00	00	00	4B	40	49	64	08	28	C3	6D	A8	40	18	47	8A	2A	90	CD	42
08A	00	00	01	2F	68	5D	F8	C0	00	0B	32	36	32	3A	31	3A	30	3A	33	33	30	FF	FF

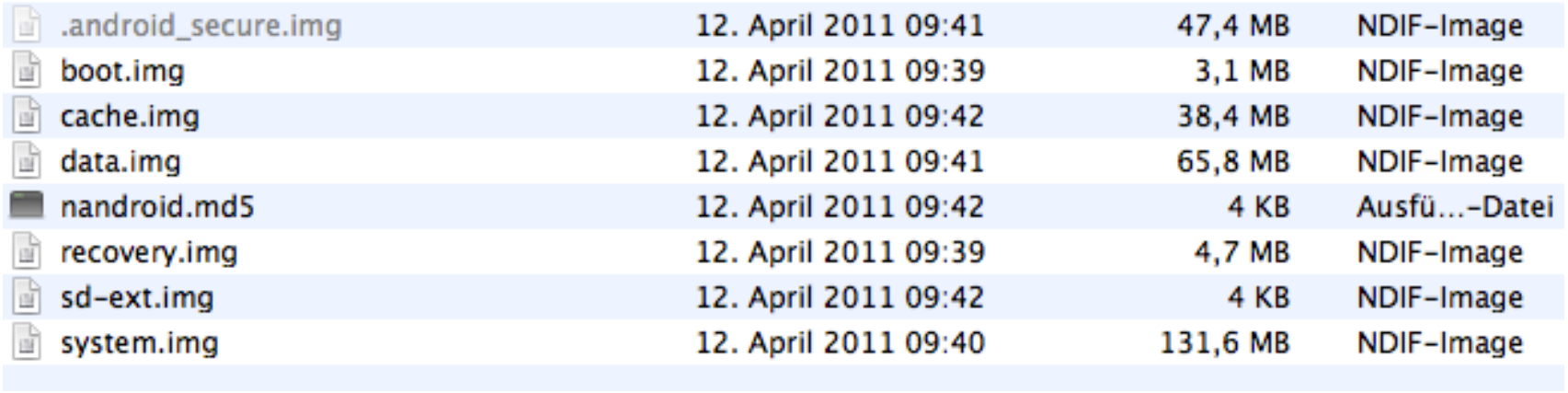
Nandroid Backup

- Mit Hilfe des Nandroid Backups kann ein Vollbackup + Hash der forensisch relevanten Daten erstellt werden
  - Nur möglich, wenn Phone gerootet ist und ein Recovery Image geflashed wurde



Nandroid Backup Vorteile

- I.d.R wird bei jedem Flashvorgang ein Backup erstellt => mehrere Backups vorhanden
- Die Sicherung kann auf der Forensik-Workstation analysiert werden



.android_secure.img	12. April 2011 09:41	47,4 MB	NDIF-Image
boot.img	12. April 2011 09:39	3,1 MB	NDIF-Image
cache.img	12. April 2011 09:42	38,4 MB	NDIF-Image
data.img	12. April 2011 09:41	65,8 MB	NDIF-Image
nandroid.md5	12. April 2011 09:42	4 KB	Ausfü...-Datei
recovery.img	12. April 2011 09:39	4,7 MB	NDIF-Image
sd-ext.img	12. April 2011 09:42	4 KB	NDIF-Image
system.img	12. April 2011 09:40	131,6 MB	NDIF-Image

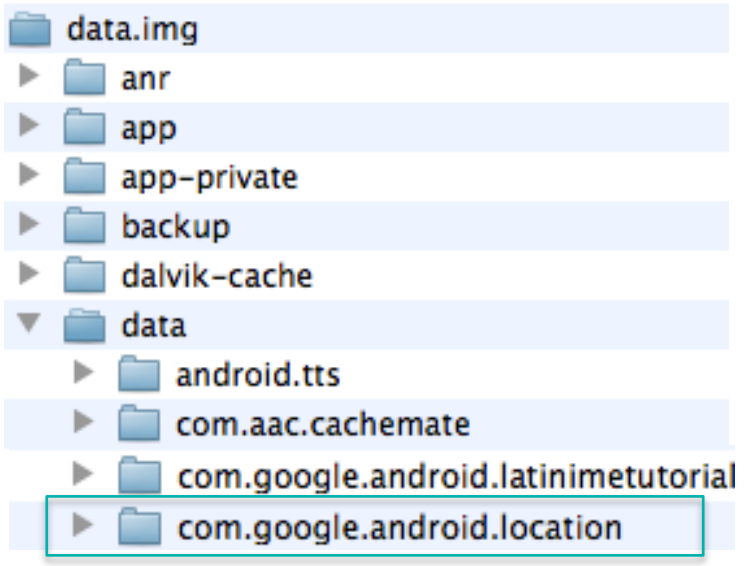
- Yaffs-Images müssen entpackt werden (unyaffs)

Nandroid Backup

Das Nandroid Backup enthält alle Daten, die auf dem NAND Flash gespeichert wurden.

Zu beachten ist:

- Reboot in RecoveryMod
- Backup wird auf Flash gespeichert



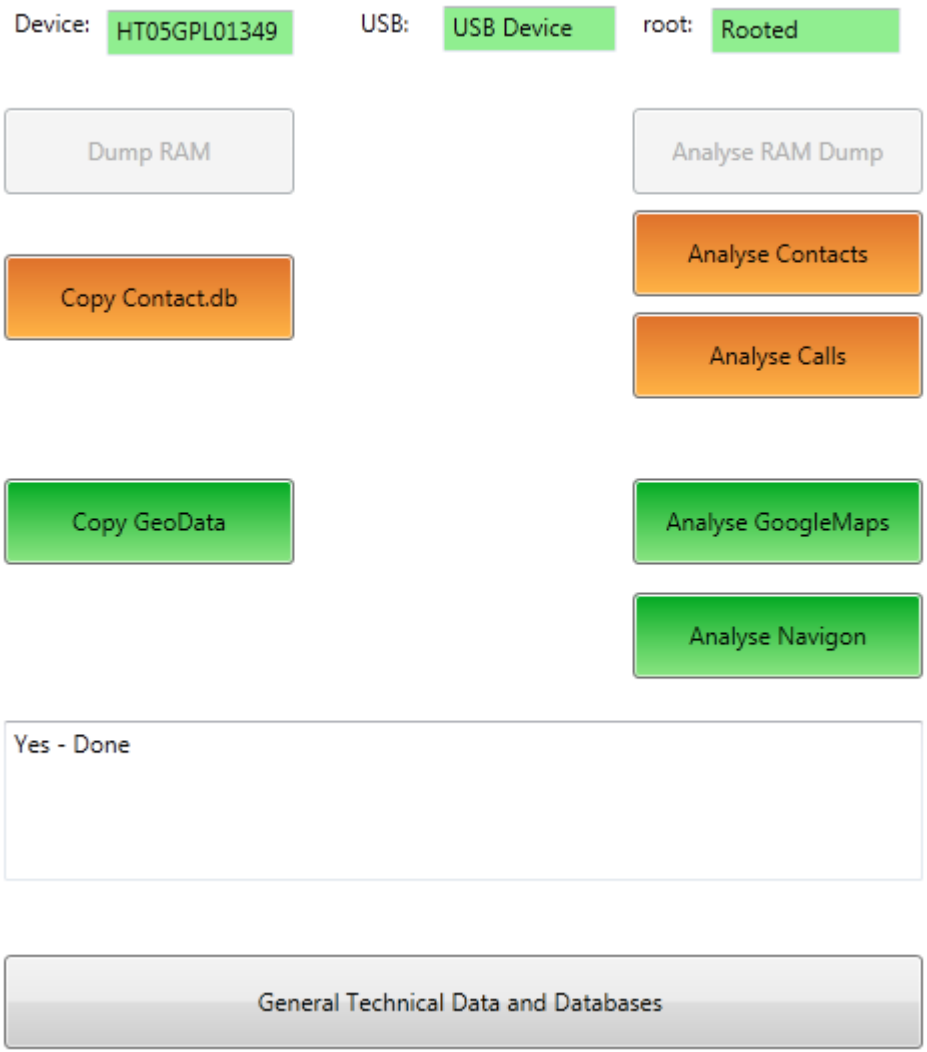
Android Forensic Toolkit

C# Toolkit zur Sicherung von forensisch relevanten Informationen

Idee:

- AFT übernimmt die Datengewinnung über die adb
- Auswertung von Standarddatenbanken
  - Kontakte, Anruflisten
  - SMS, MMS, Email
  - Passwortsuche
- Auswertung von Geodaten aus Applikationen

AFT


Device:
HT05GPL01349
USB:
USB Device
root:
Rooted
Dump RAM
Analyse RAM Dump
Analyse Contacts
Copy Contact.db
Analyse Calls
Copy GeoData
Analyse GoogleMaps
Analyse Navigon
Yes - Done
General Technical Data and Databases

Ausblick

AFT Erweiterungsmöglichkeiten durch XML Dateien

=> Jens Weidhase

Die Bachelorarbeit beschreibt die Analyse von Android und iPhone mit den genannten Software- und Hardwarelösungen im Detail.

Es werden die aktuellen Möglichkeiten und Probleme aufgezeigt.

Fazit

- Ohne Root, Extraktion nur durch App
  - Teilweise möglich ohne Reboot

- Speicherung von Geodaten

  =>detaillierte Bewegungsprofile

- Handy- und Betriebssystemvielfalt

  =>Spezialisierung auf OS

Vielen Dank für Ihre Aufmerksamkeit!

Fragen oder Anregungen?

iOS