Tools and Processes for Forensic Analyses

Android Forensics

Michael Spreitzenbarth

14.03.2013

Agenda

- Intro
- How to get the data ?
- How to crack the screen-lock ?
- Analysis of an Android smartphone
- Android Data Extractor Lite (ADEL)
- Analysis of Android applications

Intro

The Development of Smartphones and Forensics

From mobile- to smart-phone

1986

1998

today

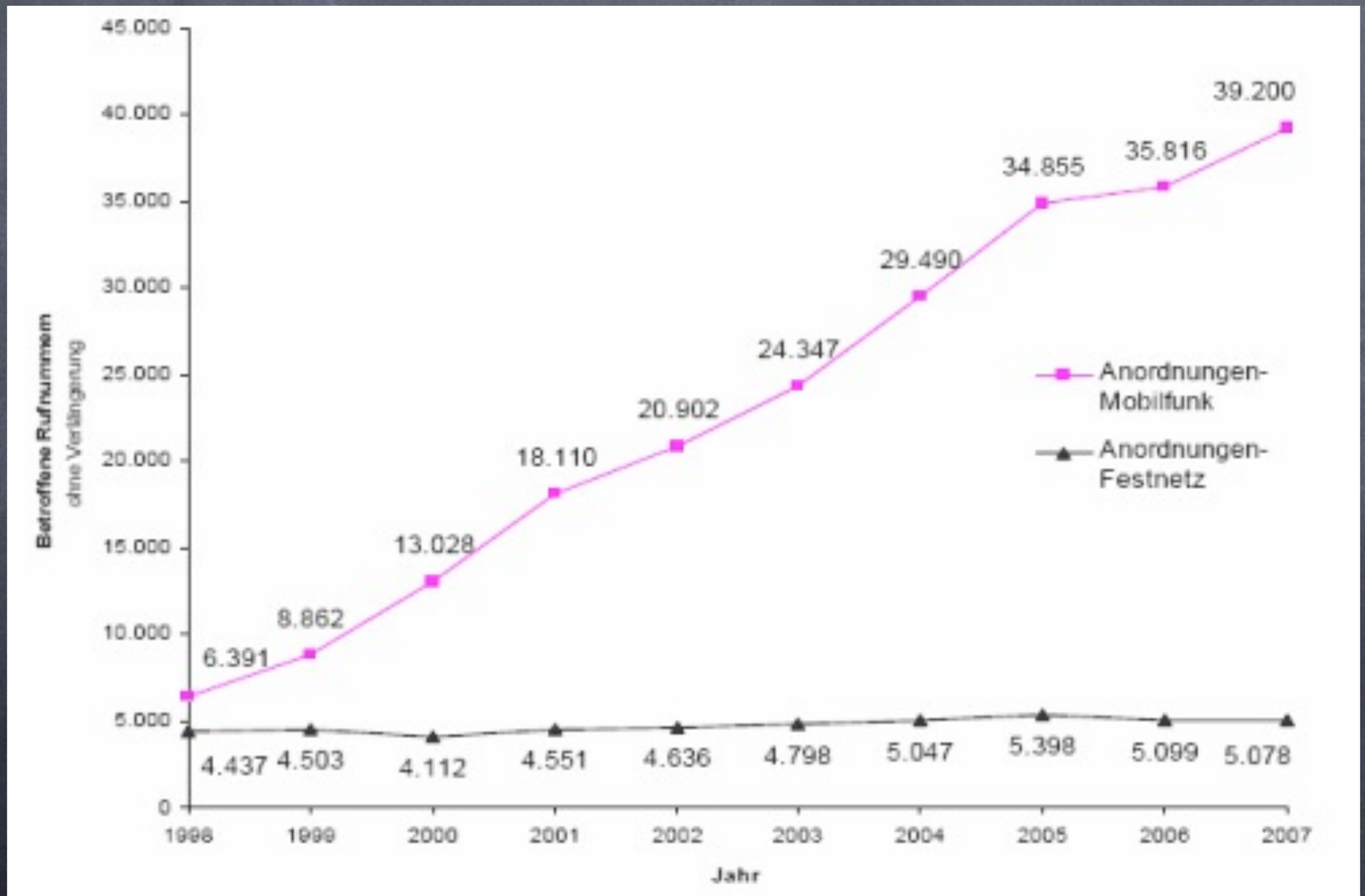
Why we choose Android ?

Worldwide Mobile Device Sales to End Users by Operating System in 3Q12 (Thousands of Units)

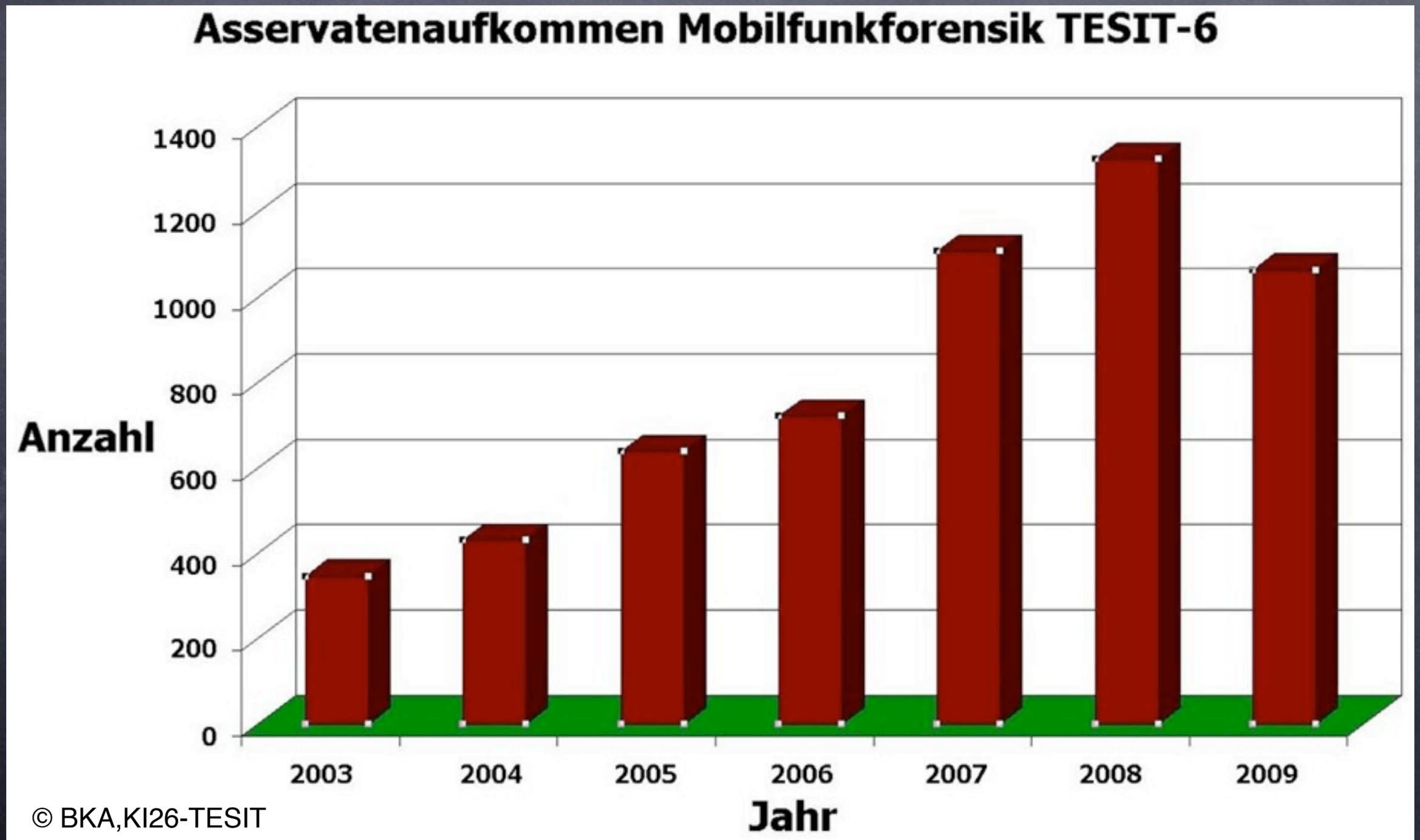
Operating System	3Q12 Units	(%)	3Q11 Units	(%)
Android	122,480.0	72.4	60,490.4	52.5
iOS	23,550.3	13.9	17,295.3	15.0
Research In Motion	8,946.8	5.3	12,701.1	11.0
Bada	5,054.7	3.0	2,478.5	2.2
Symbian	4,404.9	2.6	19,500.1	16.9
Microsoft	4,058.2	2.4	1,701.9	1.5
Others	683.7	0.4	1,018.1	0.9
Total	**169,178.6**	**100.0**	**115,185.4**	**100.0**

Source: Gartner (November 2012)

The case of mobile-phone-forensics



The case of mobile-phone-forensics



Differences in digital forensics

- unstandardized interfaces
- tools like dd not available
- its hard to get the data
- system protection measures are hard to crack

Cracking the Screenlock

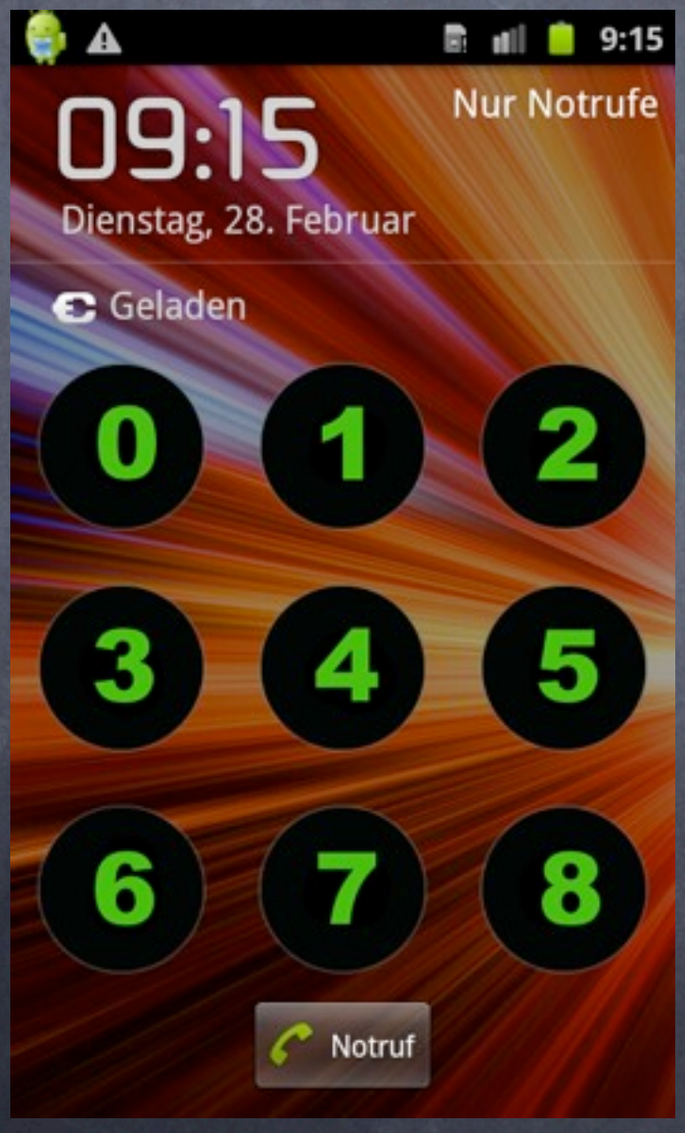
Face - Pattern - PIN

Face-Recognition

Face-Recognition

- just take a picture of the smartphone owner
- hold this picture in front of the smartphone when unlocking it

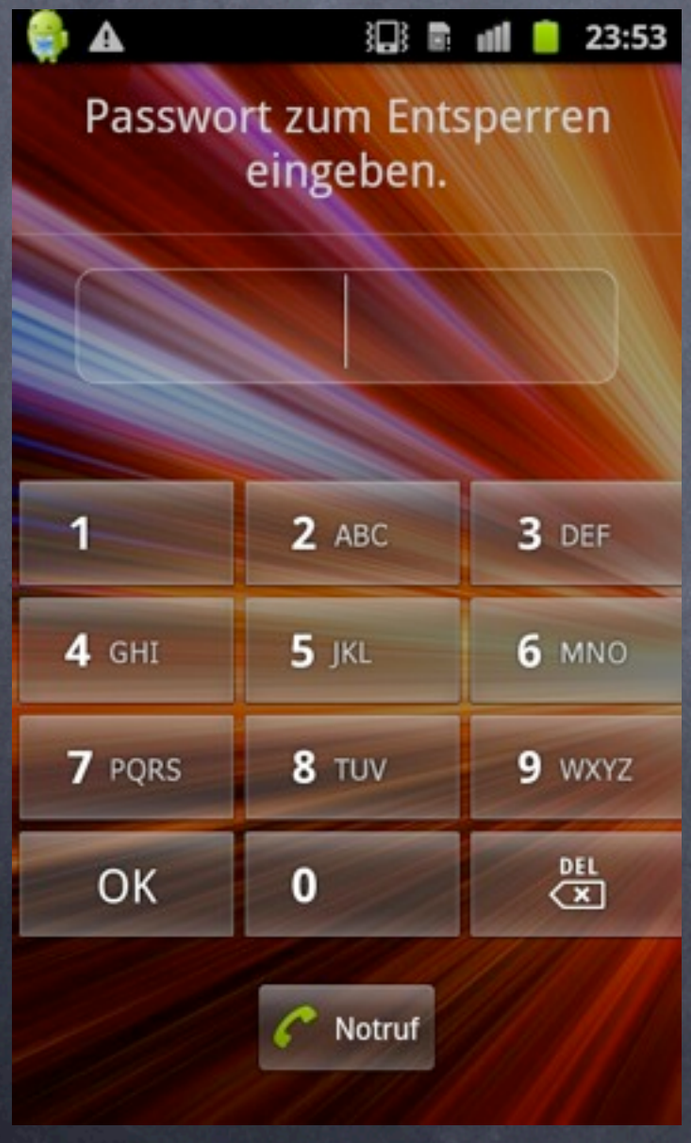
Gesture-Lock



Gesture-Lock

- the gesture is hashed with sha-1
- this hash is stored in a special file called gesture.key in /data/system/
- you can crack the gesture-lock with a rainbow-table

PIN- / Password-Lock



PIN- / Password-Lock

- PIN and Password are handled identical
- the PIN/Password is hashed with sha-1 and a salt
- this salted hash is stored in a special file called password.key in /data/system/
- the salt is stored in /data/data/com.android.providers.settings/databases/settings.db
- you can crack the screenlock by recalculating the hash (very time-consuming)

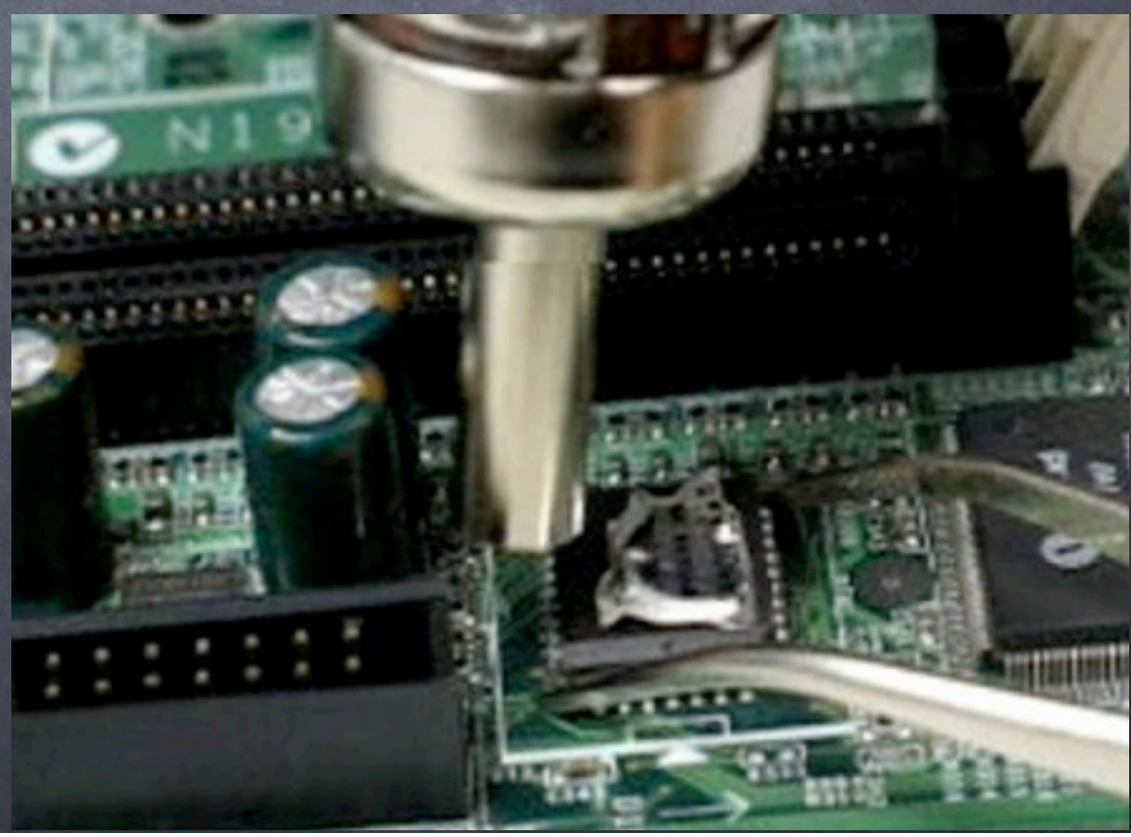
DEMO

How to get the data ?

The old and expensive Ways

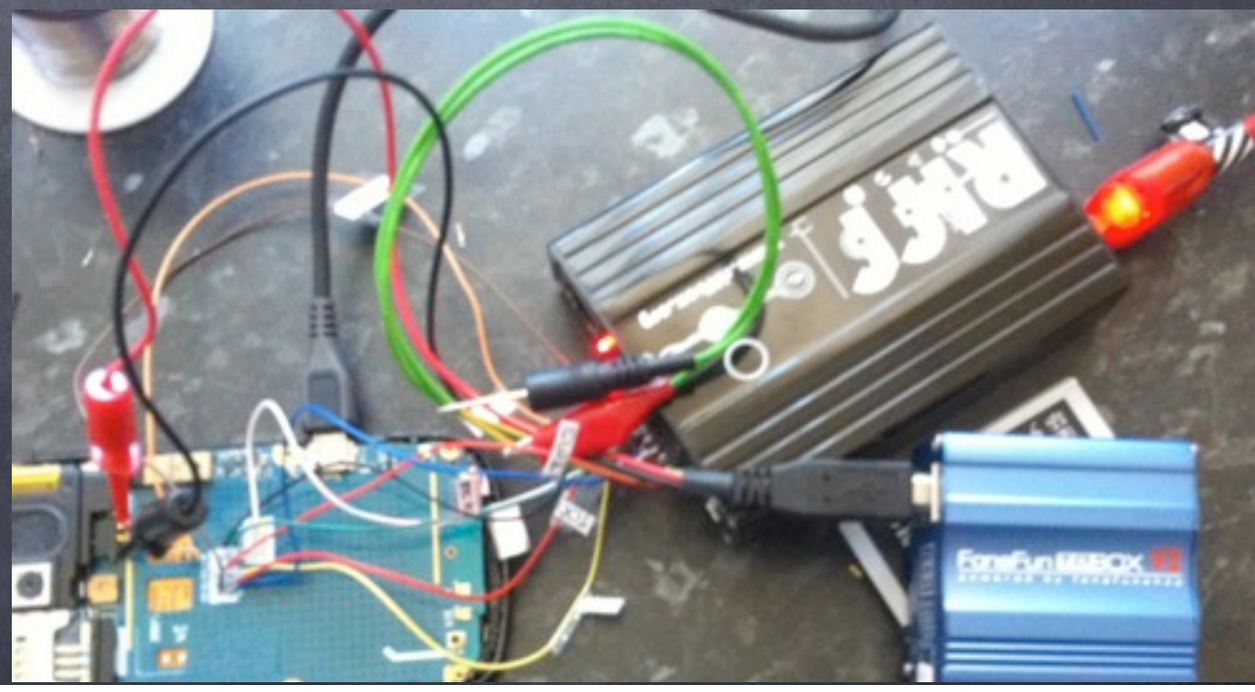
Desoldering of the memory module

- You need special and expensive hardware (about 20.000 EUR)
- high complexity
- high risk of damadge
- best results



JTAG-Interface

- not all smartphones have a JTAG-Interface
- you need special hardware (about 200 EUR)
- complex but not as riskfull as desoldering
- very good results

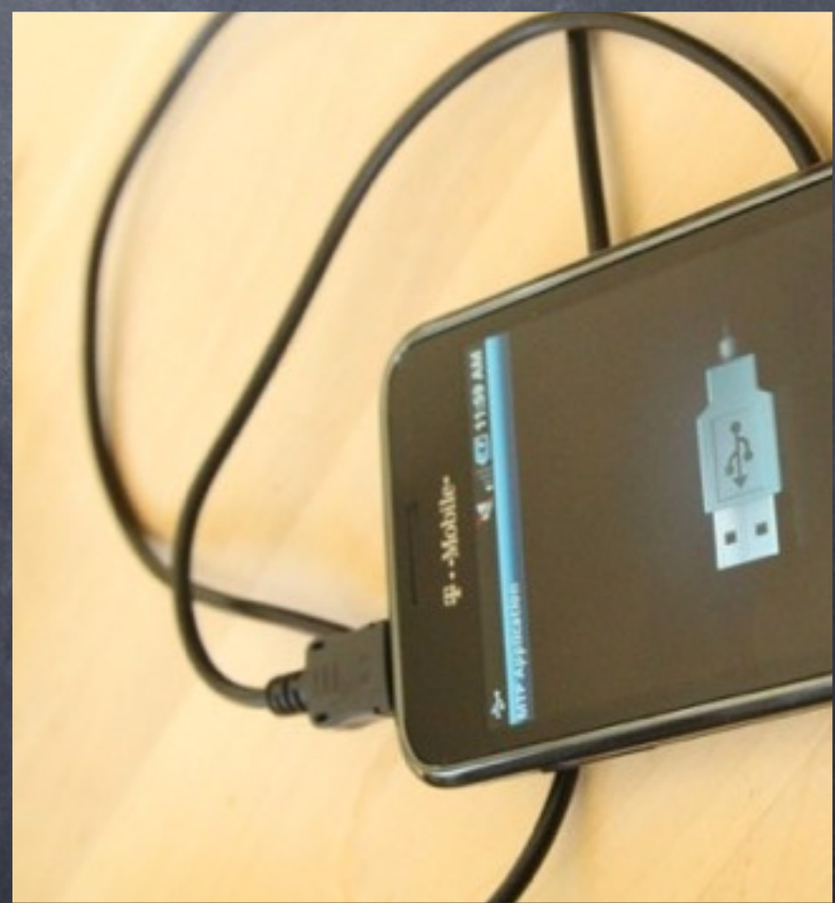


Software Agents

- SA's are apps installed directly on the device
- use permissions to get access to databases on the system
- can be fooled with the help of „shadow-databases"
- data on the smartphone gets modified
- results are not trustfully

Common Software Solutions

- Software gets installed on the investigators machine
- communicates through the data cable
- uses drivers and protocolls of the smartpone
- limited access to stored data



Forensic Analysis

Analysis of an Android Smartphone

Why getting ROOT ?

- Linux is using well known authorisation concept (users/groups)
- Android protects the application data

=> you need to be root !

All I want to be
- ROOT -

- Samsung and HTC have unlocked their bootloaders
- Exploits to unlock other/older bootloaders are in the wild (Gingerbreak, RageAgainstTheCage, etc.)

All I want to be
- ROOT -

- Flashing a new/modified kernel
- Boting into an own Recovery-Image

=> afterwards you get a root-shell

=> system protection measures can now be cracked

Where is the important data ?

- Each app has its own database (SQLite)
- The application data is located at
  - /data/data/....
  - /sdcard/data/data/....
- Documents, pictures and music is located at
  - /sdcard/....
- Each app has its own area in the RAM

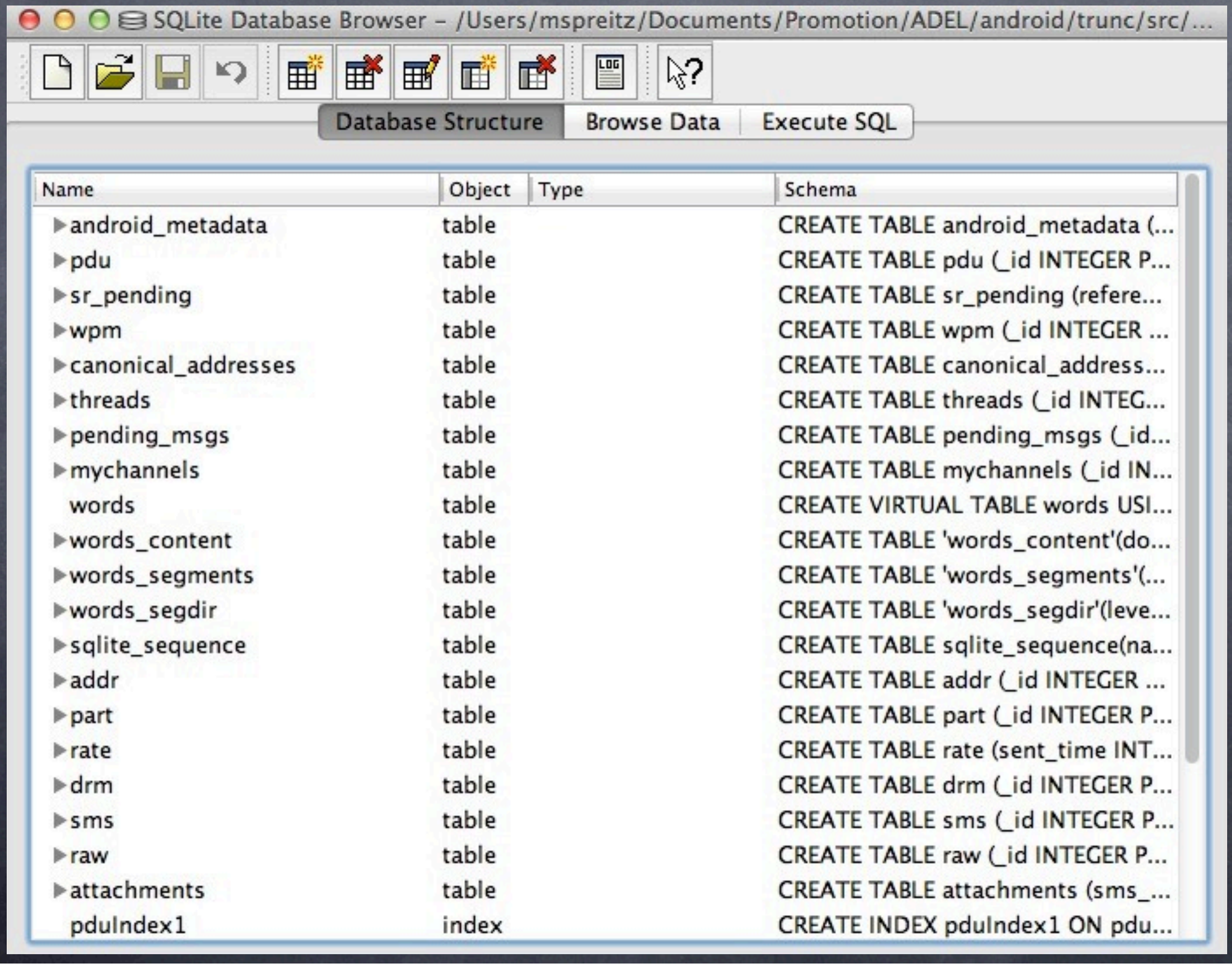
Which structure does this data has ?

- Internal Memory
  - YAFFS 2
  - EXT 4
- SD card
  - FAT / EXT 3
- RAM
  - slightly modified hprof

Which structure does this data has ?

- Pictures are JPEG
  - look for EXIF data
- Databases are SQLite
  - write your own parser
  - or use tools like:
    - SQLite Database Browser
    - Firefox SQLite Plugin

Example: SMS


SQLite Database Browser – /Users/mspreitz/Documents/Promotion/ADEL/android/trunc/src/...
Database Structure
Browse Data
Execute SQL
Name
Object
Type
Schema
android_metadata table CREATE TABLE android_metadata (...
pdu table CREATE TABLE pdu (_id INTEGER P...
sr_pending table CREATE TABLE sr_pending (refere...
wpm table CREATE TABLE wpm (_id INTEGER ...
canonical_addresses table CREATE TABLE canonical_address...
threads table CREATE TABLE threads (_id INTEG...
pending_msgs table CREATE TABLE pending_msgs (_id...
mychannels table CREATE TABLE mychannels (_id IN...
words table CREATE VIRTUAL TABLE words USI...
words_content table CREATE TABLE 'words_content'(do...
words_segments table CREATE TABLE 'words_segments'(...
words_segdir table CREATE TABLE 'words_segdir'(leve...
sqlite_sequence table CREATE TABLE sqlite_sequence(na...
addr table CREATE TABLE addr (_id INTEGER ...
part table CREATE TABLE part (_id INTEGER P...
rate table CREATE TABLE rate (sent_time INT...
drm table CREATE TABLE drm (_id INTEGER P...
sms table CREATE TABLE sms (_id INTEGER P...
raw table CREATE TABLE raw (_id INTEGER P...
attachments table CREATE TABLE attachments (sms_...
pduIndex1 index CREATE INDEX pduIndex1 ON pdu...

Example: SMS

	_id	thread_id	address	perso	date	protocol	read
1	1	1	3Alerts		946884213134	0	
2	2	1	3Alerts		946884245833	0	
3	3	1	3Alerts		1312572952989	0	
4	4	2	Rate Advice		1312572963616	0	
5	5	3	SWISSCOM		1312742754973	57	
6	6	4	Swisscom		1312742856733	57	
7	7	5	801		1312742978556	57	
8	8	5	801		1312800462737	57	
9							
10							
11							

	body	service_center	locke
1	Please keep your phone on while we connect you to Three. It'll take abo	+447782000801	
2	We've nearly finished. Now we just need you to turn your phone off and	+447782000801	
3	If you now need to, top-up £15 & buy All in One 15 Add-on to get 300	+447782000801	
4	From 3: In EU it's max of 36.6p/min to call,11.5p/min to receive call,10	+447782000801	
5	Tarife (CHF) in Europa: Anrufe innerhalb Europa und in die Schweiz: 0.8!	+41794999000	
6	Damit Sie Ihre NATEL-Dienste optimal verwenden können, erhalten Sie	+41794999000	
7	Unser Geschenk: Sie erhalten ein NATEL easy Datenpaket 100 MB für die	+41794999000	
8	Aufgeladener Betrag: CHF 30.00 Neues Guthaben: CHF 38.71 Sie könne	+41794999000	
9	Sie haben noch 18 MB vom NATEL easy Datenpaket zur Verfügung. Sie k	+41794999000	
10	Sie haben noch 8 MB vom NATEL easy Datenpaket zur Verfügung. Sie kö	+41794999000	
11	Ihr NATEL easy Datenpaket DATA100MB ist abgelaufen oder aufgebrauc	+41794999000	

Example: JPEG

- EXIF data of a JPEG file:
  - Location of the picture (GPS)
  - Camera type
  - timestamp

Example: JPEG

Basic Image Information

Camera:	Apple iPhone 4
Lens:	3.9 mm Digital Zoom: 2.347432024×
Exposure:	Auto exposure, Program AE, 1/17 sec, f/2.8, ISO 80
Flash:	Off, Did not fire
Date:	**May 22, 2011** 2:50:02PM (6 months, 7 days, 7 hours, 7 mi ahead of GMT)
Location:	Map via encoded GPS coordinat (also see the Google Maps pane Timezone guess from earthtools
File:	**1,936 × 2,592** JPEG (**5.0** m 1,345,625 bytes (1.3 megabytes)

GPS-encoded location: 49° 30' 04"N, 10° 58' 07"E
Map center: 49° 30' 04"N, 10° 58' 07"E

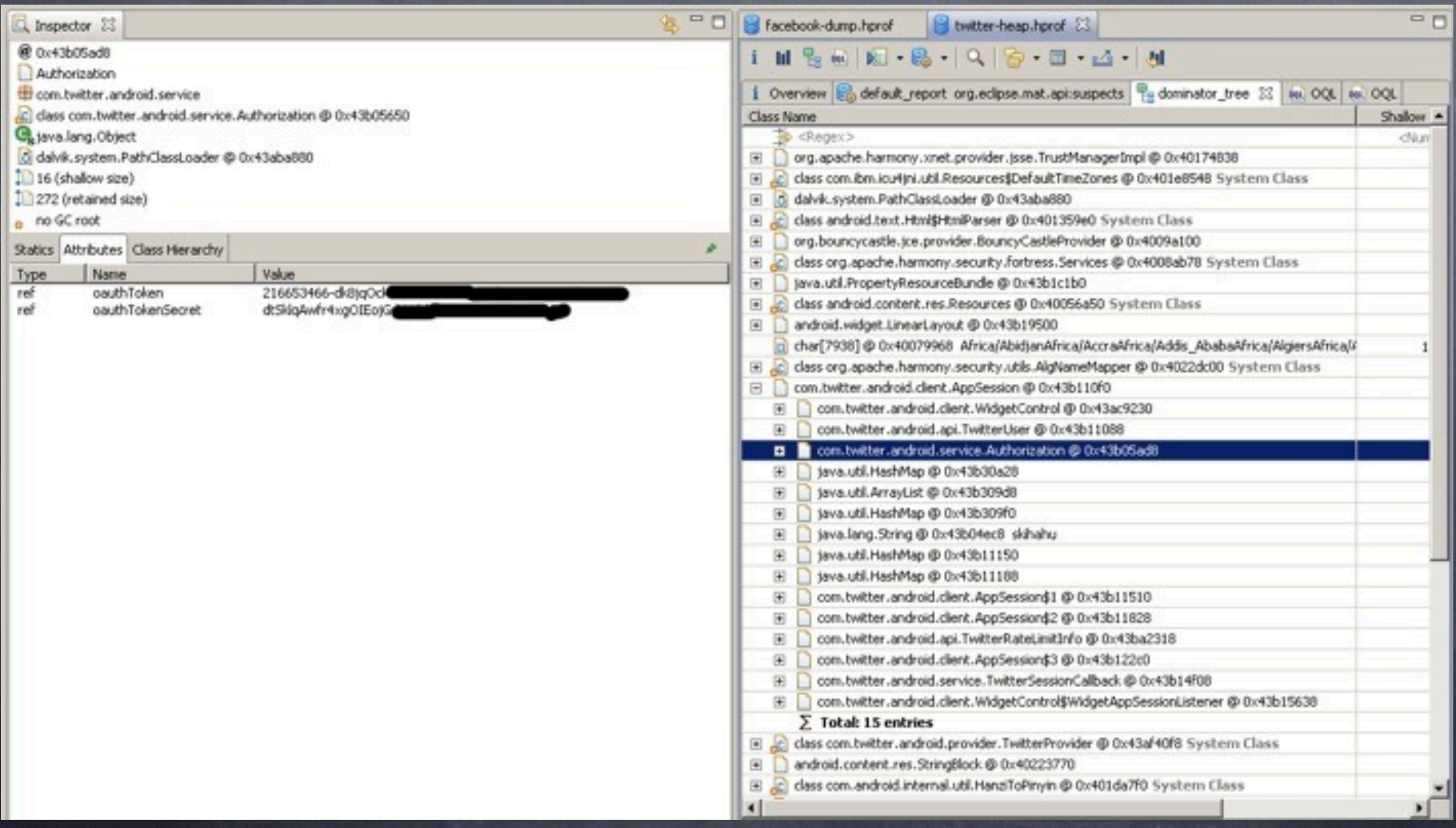
Display area: 970 m × 349 m
Distance between: 0 m

Click on map to measure distance from GPS-encoded location

Example: RAM

- until Android 2.3
  - kill -10 <pid>
- since Android 2.3
  - Dalvik Debug Monitor Server (DDMS)

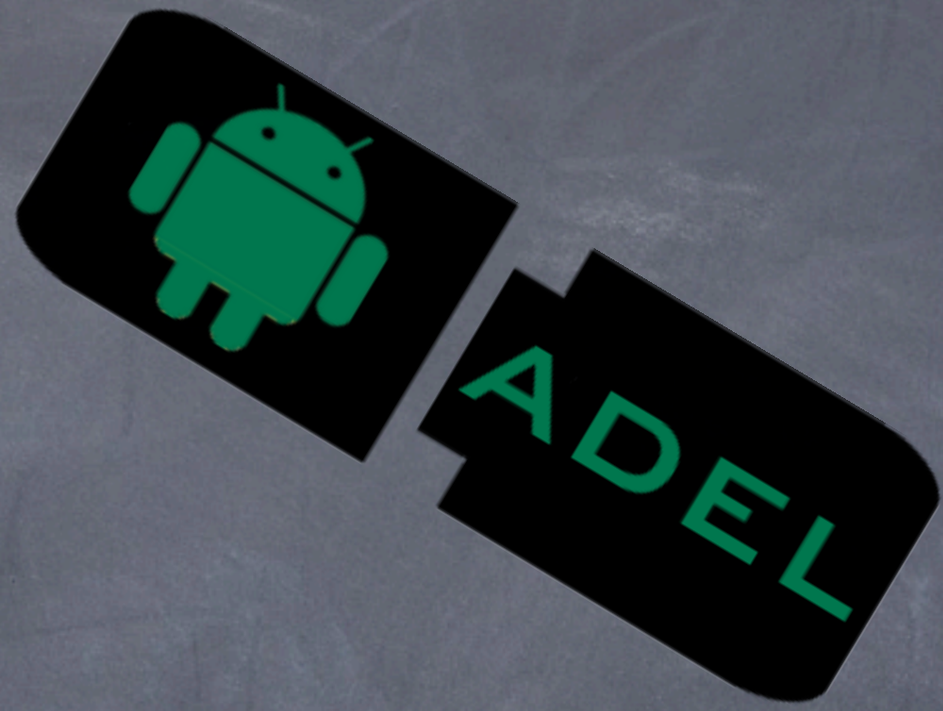
Example: RAM


Inspector
0x43b05ad8
Authorization
com.twitter.android.service
class com.twitter.android.service.Authorization @ 0x43b05650
java.lang.Object
dalvik.system.PathClassLoader @ 0x43aba880
16 (shallow size)
272 (retained size)
no GC root
Statics
Attributes
Class Hierarchy
Type
Name
Value
ref
oauthToken
ref
oauthTokenSecret
facebook-dump.hprof
twitter-heap.hprof
Overview
default_report org.eclipse.mat.api:suspects
dominator_tree
OQL
OQL
Class Name
Shallow
<Regex>
org.apache.harmony.xnet.provider.jsse.TrustManagerImpl @ 0x40174838
class com.ibm.icu4jni.util.Resources$DefaultTimeZones @ 0x401e8548 System Class
dalvik.system.PathClassLoader @ 0x43aba880
class android.text.Html$HtmlParser @ 0x401359e0 System Class
org.bouncycastle.jce.provider.BouncyCastleProvider @ 0x4009a100
class org.apache.harmony.security.fortress.Services @ 0x4008ab78 System Class
java.util.PropertyResourceBundle @ 0x43b1c1b0
class android.content.res.Resources @ 0x40056a50 System Class
android.widget.LinearLayout @ 0x43b19500
char[7938] @ 0x40079968 Africa/AbidjanAfrica/AccraAfrica/Addis_AbabaAfrica/AlgiersAfrica/
class org.apache.harmony.security.utils.AlgNameMapper @ 0x4022dc00 System Class
com.twitter.android.client.AppSession @ 0x43b110f0
com.twitter.android.client.WidgetControl @ 0x43ac9230
com.twitter.android.api.TwitterUser @ 0x43b11088
com.twitter.android.service.Authorization @ 0x43b05ad8
java.util.HashMap @ 0x43b30a28
java.util.ArrayList @ 0x43b309d8
java.util.HashMap @ 0x43b309f0
java.lang.String @ 0x43b04ec8 skihahu
java.util.HashMap @ 0x43b11150
java.util.HashMap @ 0x43b11188
com.twitter.android.client.AppSession$1 @ 0x43b11510
com.twitter.android.client.AppSession$2 @ 0x43b11828
com.twitter.android.api.TwitterRateLimitInfo @ 0x43ba2318
com.twitter.android.client.AppSession$3 @ 0x43b122c0
com.twitter.android.service.TwitterSessionCallback @ 0x43b14f08
com.twitter.android.client.WidgetControl$WidgetAppSessionListener @ 0x43b15638
Total: 15 entries
class com.twitter.android.provider.TwitterProvider @ 0x43af40f8 System Class
android.content.res.StringBlock @ 0x40223770
class com.android.internal.util.HanziToPinyin @ 0x401da7f0 System Class

Android Data Extractor Lite

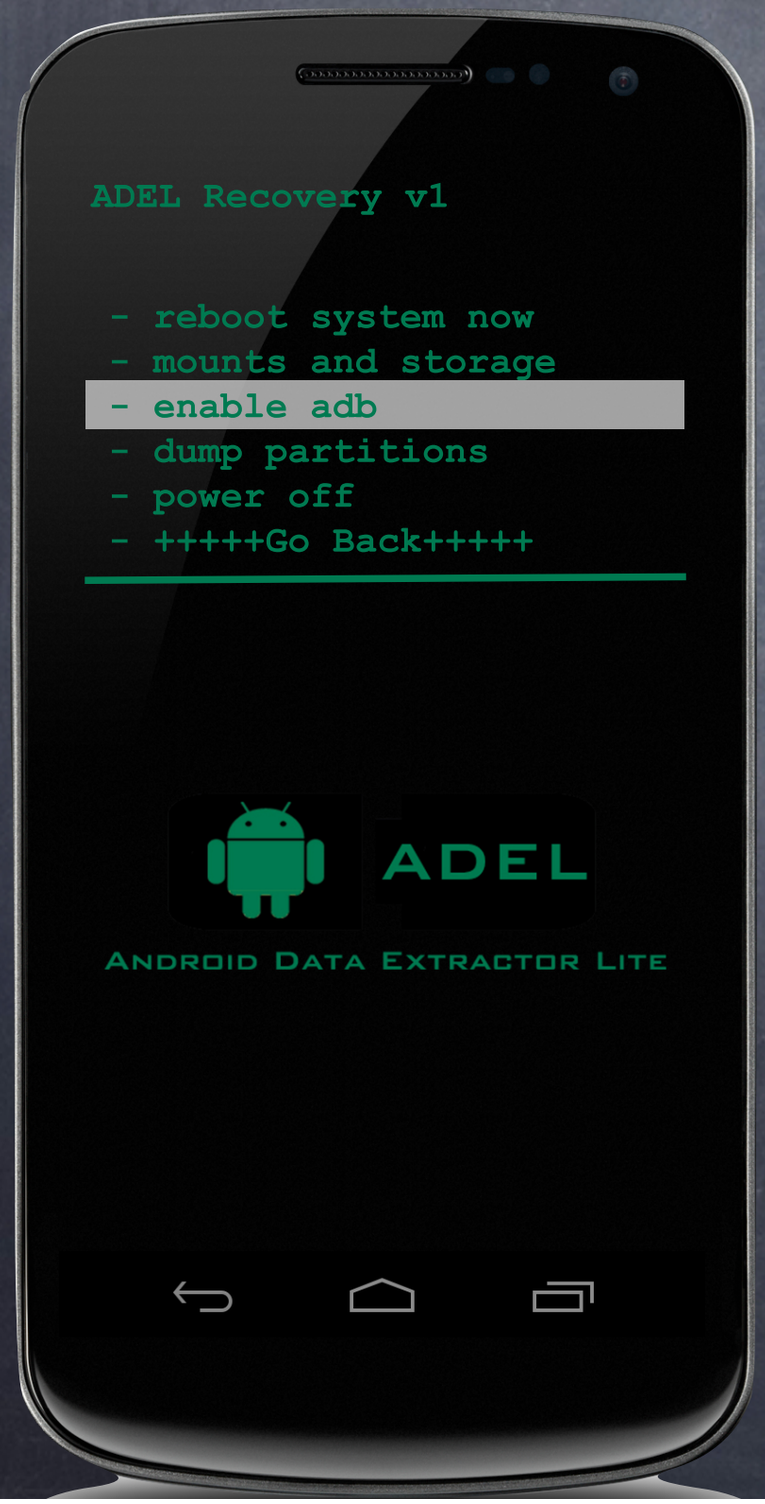
Automated Smartphone Analysis

What is ADEL ?



- A fully automated tool to forensically analyze Android smartphones
- Python based
- Unitized layout
- Analyzes databases of well known apps
- Extracts EXIF data from JPEG files
- Generates movement-profiles
- Works on Linux and Mac OS X

Recovery-Image

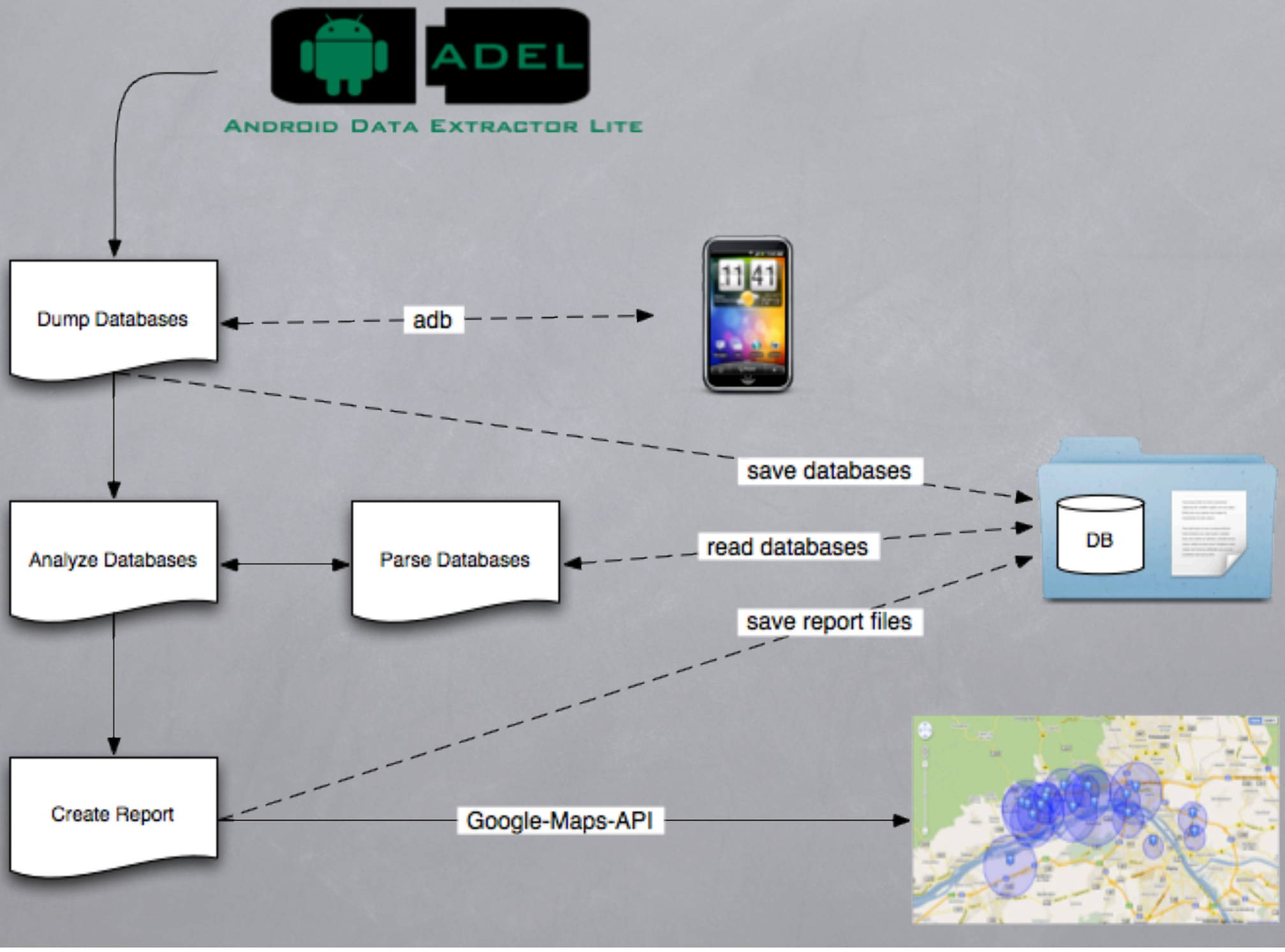


- root shell
- enable/disable adb
- create dd dump of any partition
- mount/unmount partitions
- loadable in RAM with the help of fastboot

open-source version is available on:

https://github.com/mspreitz/ADEL

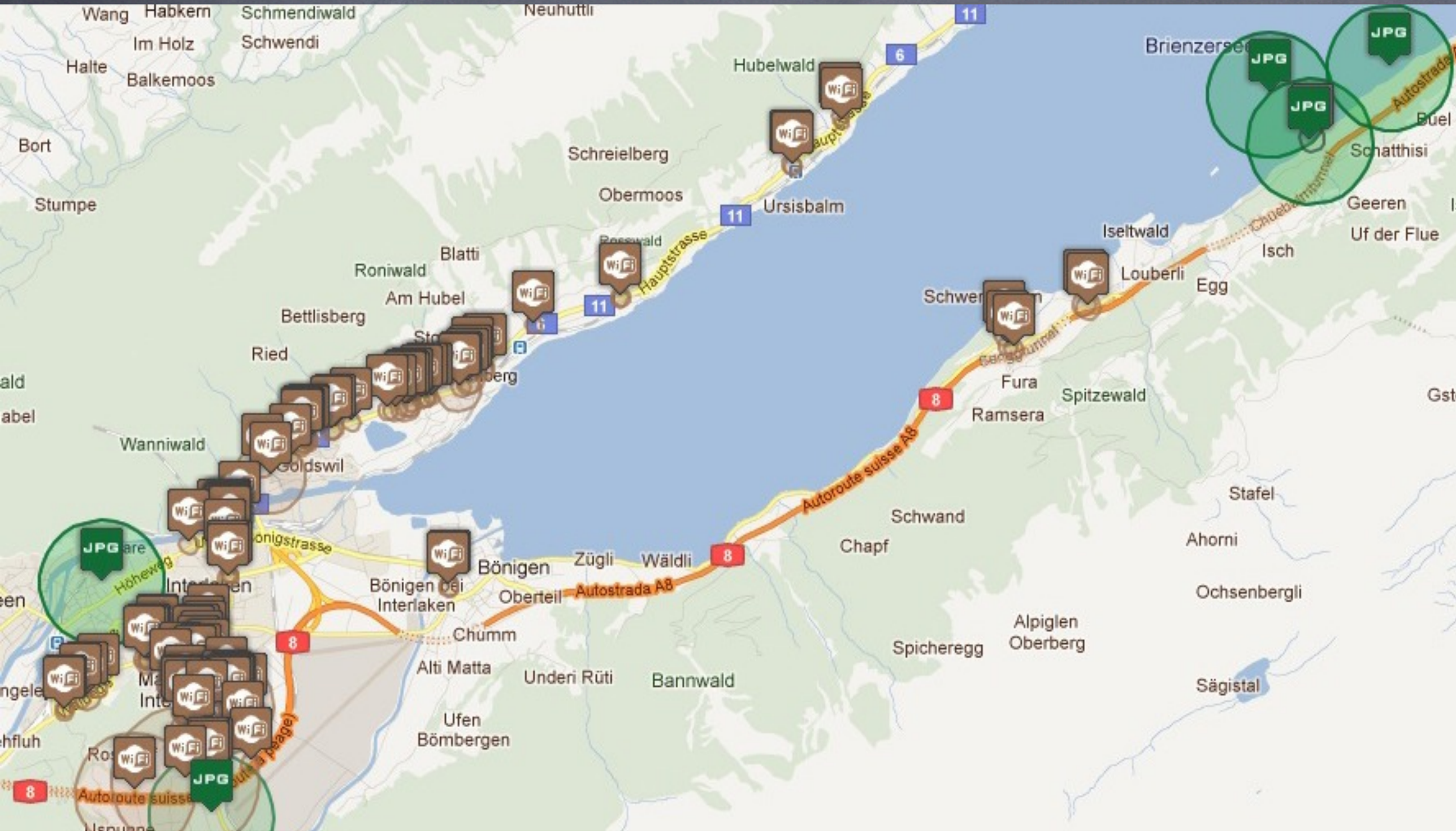
Workflow


ADEL
Android Data Extractor Lite
Dump Databases
adb
save databases
Analyze Databases
Parse Databases
read databases
DB
save report files
Create Report
Google-Maps-API

Movement-Profiles

- Most of the apps store location data
- Android has its own cache files for wifi and cell related location data
- Even widgets store location data
- GoogleMaps stores navigations
- The browser stores local search results

Movement-Profiles



DEMO

Analysis of Android Applications

Android Malware

Android Malware

- we analyzed over 300.000 apps from official and in-official market-places
- we found over 44.000 malicious applications
- even some zero-days
- we clustered them into 152 malware-families

- Families that steal personal information 51,3 %
- Families that send premium rated SMS messages 30,1 %
- Families with characteristics of a Botnet 23,5 %
- Families that contain Root-Exploits 18,3 %
- Families downloaded from the Google-Play Market 11,3 %
- Families that install additional applications 10,4 %
- Families that steal location related data 8,7 %
- Potentially unwanted applications 7,8 %
- Online-Banking Trojans 3,5 %

How do apps look like?

- META-INF: directory containing certificates
- lib: directory containing the compiled code that is specific to a software layer of a processor
- resources.arsc: a file containing pre-compiled resources
- res: directory containing resources not compiled into resources.arsc
- AndroidManifest.xml: an additional manifest file with meta-information of the application
- classes.dex: the compiled classes in the dex file format

Which tools do I need?

- Android SDK (aapt)
- dex2jar
- JD-GUI

DEMO

Thank You for Your Attention !

Michael Spreitzenbarth

Chair for IT Security Infrastructures

University of Erlangen-Nuremberg

91058 Erlangen-Tennelohe

michael.spreitzenbarth@cs.fau.de

forensics.spreitzenbarth.de