Tools and Processes for Forensic Analyses of Smartphones and Mobile Malware

Michael Spreitzenbarth

March 21st 2011

Agenda

- About the Project
- Introduction
- Android Forensics
  - ADEL & Panoptes
- Mobile Malware
- Further Work

About MobWorm

- Aims of the project:
  - Development of forensic methods and tools
  - Development of mobile Honeypots / Honeynets
  - Development of mobile Sandbox
  - POC of attack and defense scenarios
- Participants:
  - Ruhr University Bochum
  - University of Erlangen-Nuremberg
  - G-Data
  - Recurity Labs

Bundesministerium
für Bildung
und Forschung

Why Android ?

- Open Source mobile OS
- Biggest growth rate in sector
- Many different manufacturers
- Many different fields of application (smartphone, tablet, TV......)
- According to the leading market research companies THE mobile OS of the future

Top Smartphone Platforms
3 Month Average

Market-Share (%) of Smartphone Subscribers

	January 2011	
	US	Europe
Apple	24,7	20,0
Google	***31,2***	24,3
Microsoft	8,0	13,7
Palm	3,2	--
RIM	30,4	15,0
Symbian	--	***27,0***

Source: comScore MobiLens & IDC European Quarterly Mobile Phone Tracker

Android Forensics

- Security restrictions of the Android platform
- SQLite databases
- Filesystem:
    - YAFFS2
    - EXT4

Android Forensics

Panoptes

Software-Agent

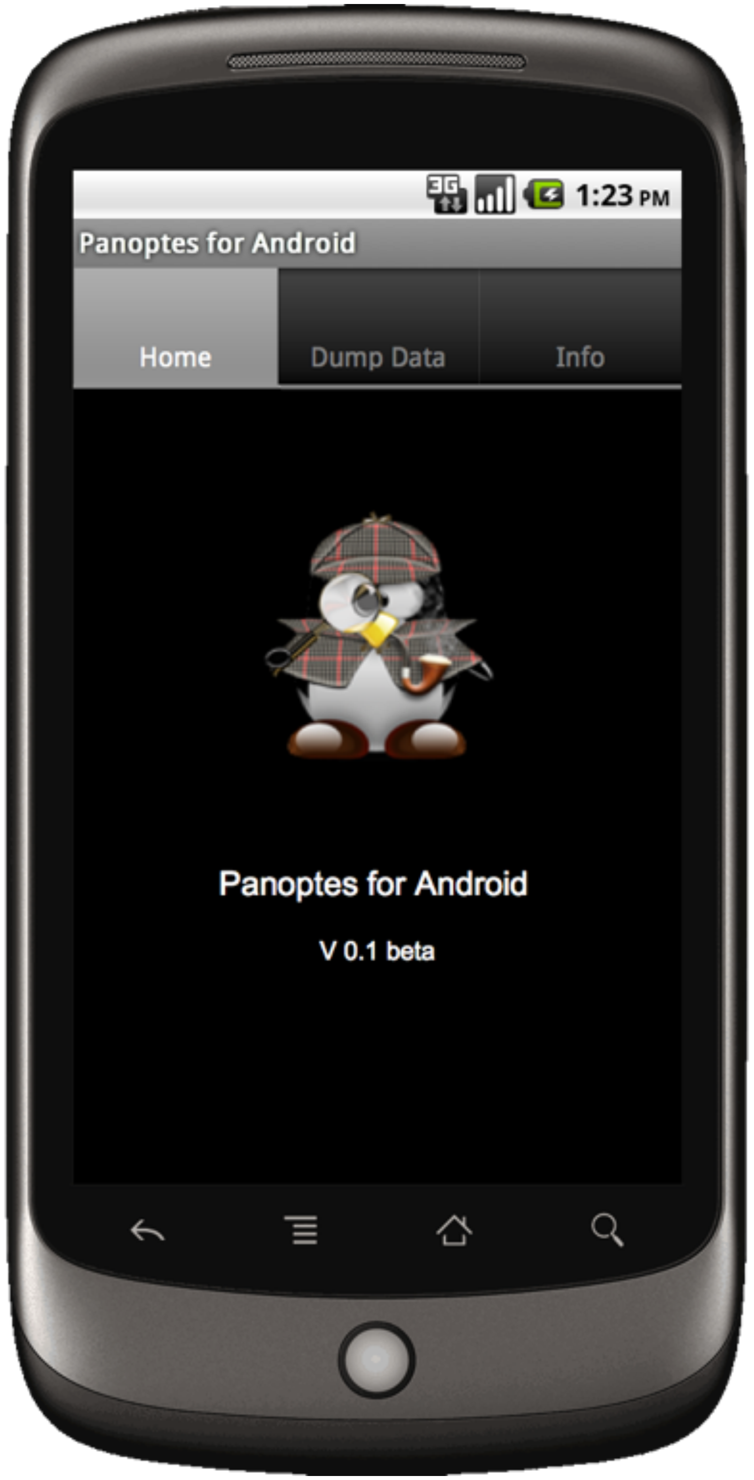
ADEL

„Forensic“ Software

Panoptes

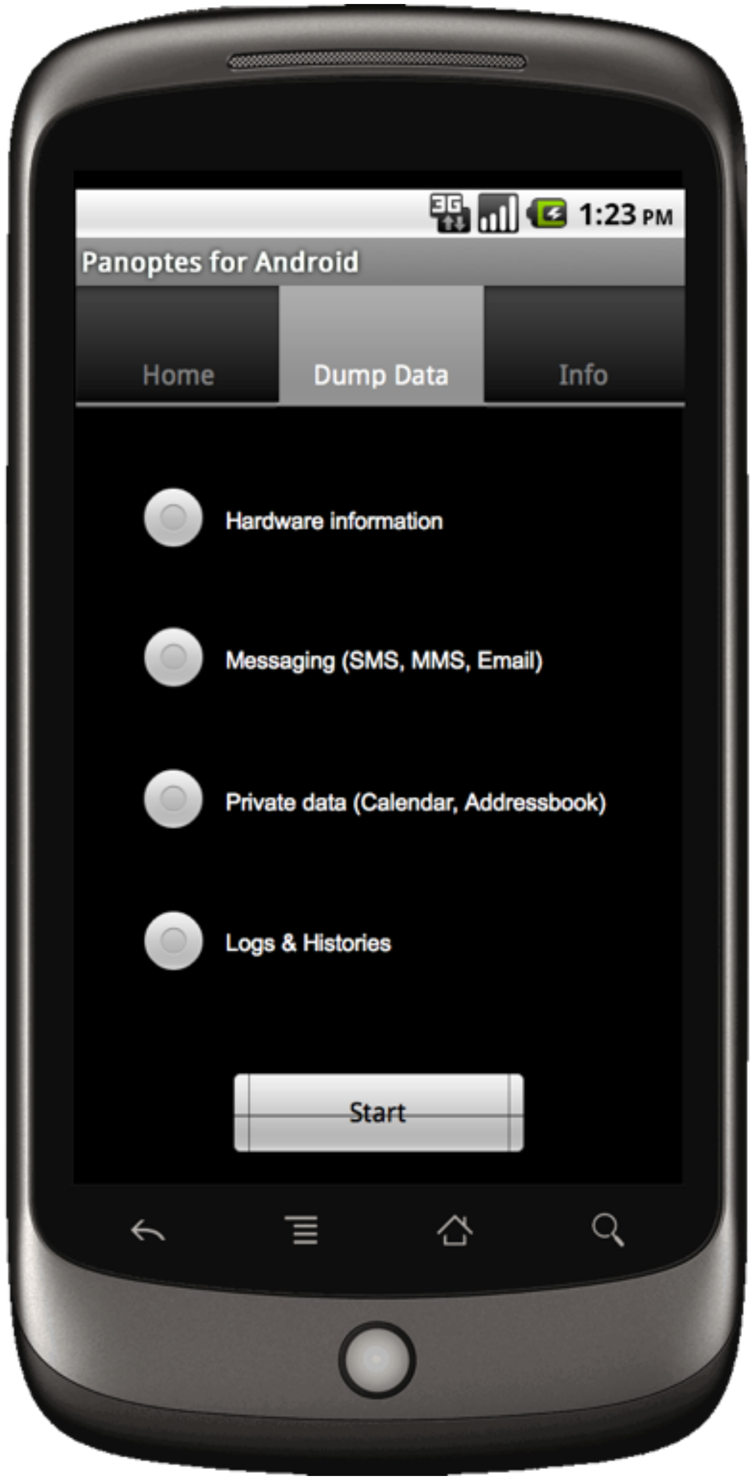
- Software Agent (on-phone-toolkit)
- JAVA App
- Uses Content Provider to access the databases
- Generates CSV-files

- Has to be installed on the device



Panoptes for Android

V 0.1 beta



○ Hardware information

○ Messaging (SMS, MMS, Email)

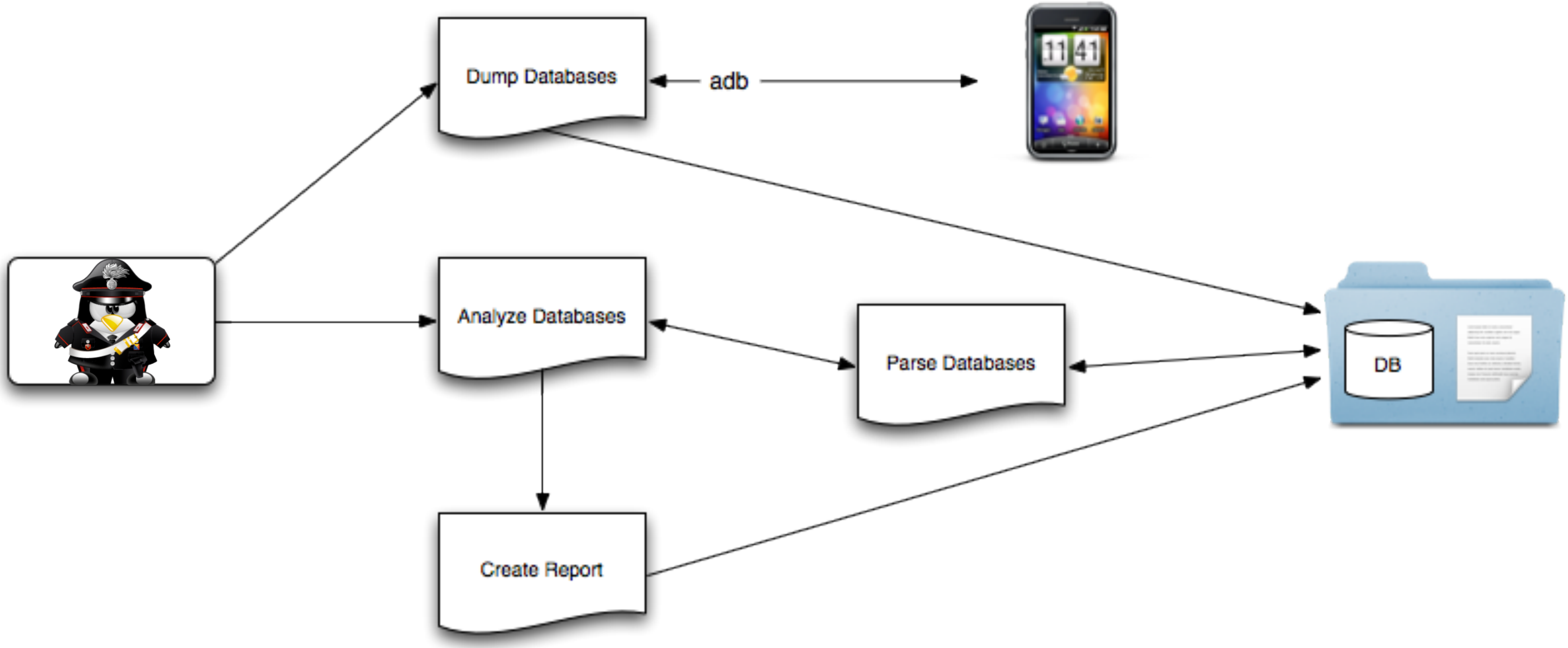
○ Private data (Calendar, Addressbook)

○ Logs & Histories

ADEL

(Android Data Extractor Lite)

- Modular design
- Connection through adb
- Dumps SQLite databases
- Uses its own SQLite parser
- Generates XSL / XML report


Dump Databases
adb
Analyze Databases
Parse Databases
DB
Create Report

Forensic Analysis of Smartphones: The Android Data Extractor Lite

Felix Freiling, Michael Spreitzenbarth, Sven Schmitt

Conference on Digital Forensics, Security and Law

Richmond, Virginia, USA
May 25-27, 2011

Terminal — adb — 100×25

```
dumpDBs:          ----> opening connection to device: emulator-5554
                                                         5554 created
                                                         del.log created
```

```
Android Data E

############  SMARTPHONE

dumpDBs:              Date
dumpDBs:              Devi
dumpDBs:              Devi
dumpDBs:              CID
dumpDBs:              Log

############  DUMP SQLite

accounts.db -> 16384 byte
contacts2.db -> 458752 by
mmssms.db -> 125952 bytes
calendar.db -> 204800 bytes in 0.114s -> 621e7f0028c64fcb53c98f2057078


############  SQLite PARSER -> 2011-02-06__16-47-39__HT98MKF00143/data
```

or Lite

model	android version
HTC Magic	Android 2.2

Contact Entries

Mobile Malware

- Smartphones have powerful hardware
- First malware sighted:
    - ZeuS-MITMO
    - DroidDream
    - zHash
- Only few detection processes
- Nearly no defensive measures

Mobile Sandbox

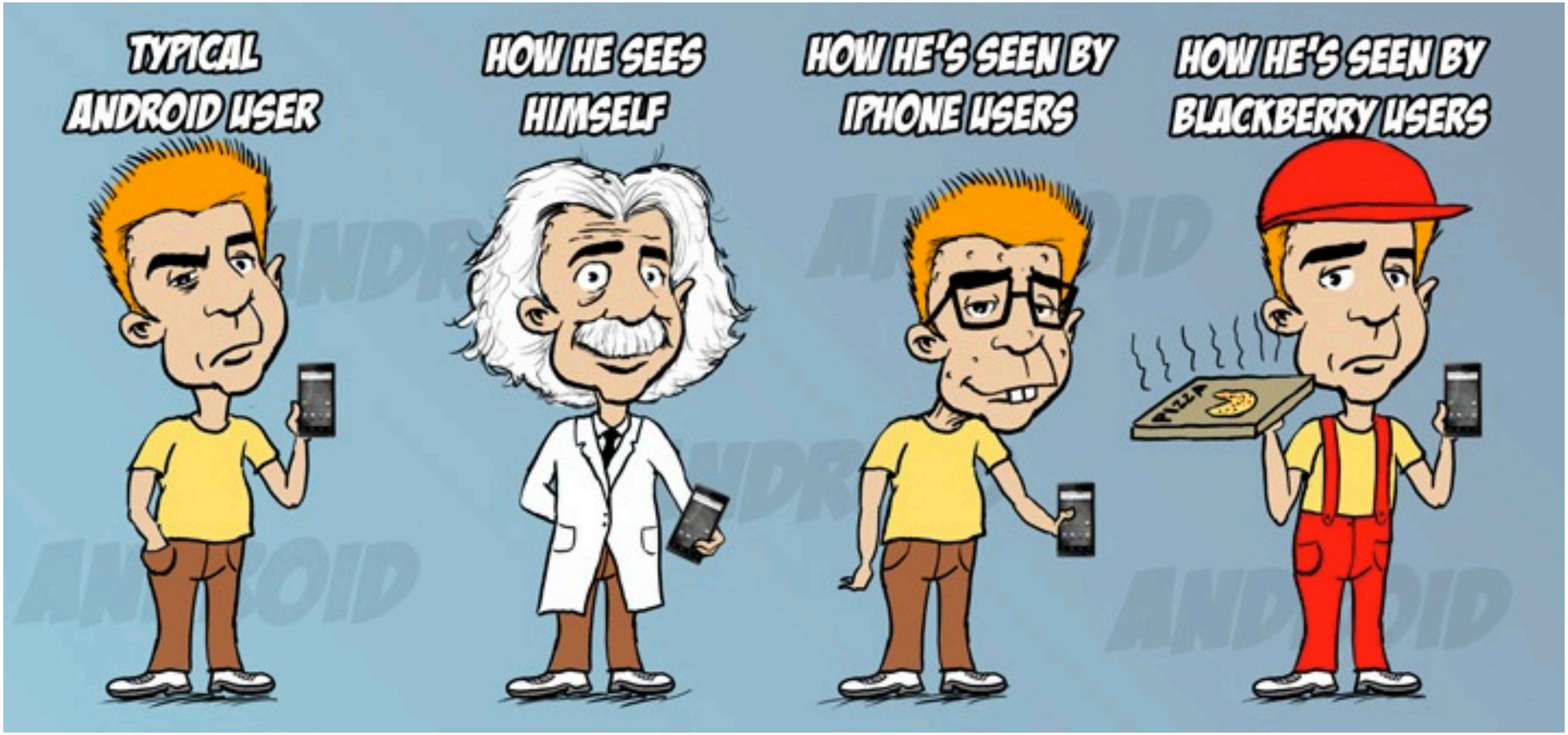
- Android based sandbox for malware analysis
- Fully automated analysis process and reporting

- Is it possible to adopt known approaches?
  - CWSandbox or MobileSandbox
  - pTrace or sTrace
  - sebek

Further Work

- Creation of forensic tools and procedures for YAFFS2 and EXT4
- Increased functionality of ADEL
- Analyze and „understand“ Android malware
- Building a Mobile Sandbox for Android

Questions ?


TYPICAL ANDROID USER
HOW HE SEES HIMSELF
HOW HE'S SEEN BY IPHONE USERS
HOW HE'S SEEN BY BLACKBERRY USERS
PIZZA
ANDROID

Thank you very much for your Attention

- Michael Spreitzenbarth
- Chair for IT Security Infrastructures
- University of Erlangen-Nuremberg
- 91058 Erlangen-Tennelohe
- michael.spreitzenbarth@informatik.uni-erlangen.de

References

- F. Freiling, S. Schmitt, and M. Spreitzenbarth, „Forensic Analysis of Smartphones: The Android Data Extractor Lite (ADEL)" in Conference on Digital Forensics, Security and Law, 2011.

- T. Holz, F. Freiling, C. Willems, „Toward Automated Dynamic Malware Analysis Using CWSandbox" in 3th European Wireless Conference, 2007

- M. Becher, „MobileSandbox", http://mobilesandbox.org

- TuX-Logos from the website http://tux.crystalxp.net/

- iPhone vs. Android vs. BlackBerry from the website http://www.csectioncomics.com/2010/11/iphone-vs-android-vs-blackberry.html