BIRMINGHAM CITY University

Mobile Forensics

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

The Higher Education Academy

BIRMINGHAM CITY University

Outline

- Introduction
- Type of extracted data
- Example scenarios of data recovery
- Summary

BIRMINGHAM CITY University

Introduction

- Convergence of mobile operating systems
- Mobile/light version of dominant operating systems
  - Linux → Android
  - Mac OS → iOS
  - Windows
  - Blackberry
- Old mobile phones are still running of proprietary operating systems
  - Symbian, Bada (바다), Palm OS, …
- Analysis of data, connectivity, location, etc.

ZEIT ONLINE | DATENSCHUTZ

BIRMINGHAM CITY University

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE

Start › Digital › Datenschutz › Data Protection: Betrayed by our own data

DATA PROTECTION

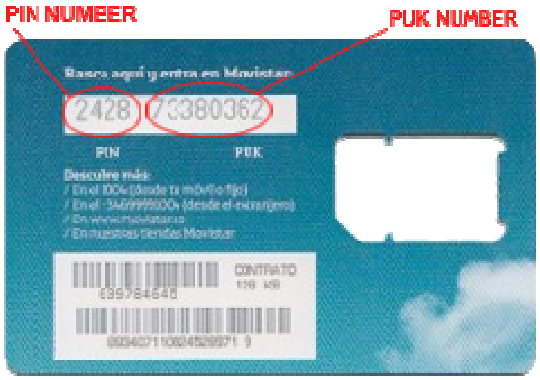
Betrayed by our own data

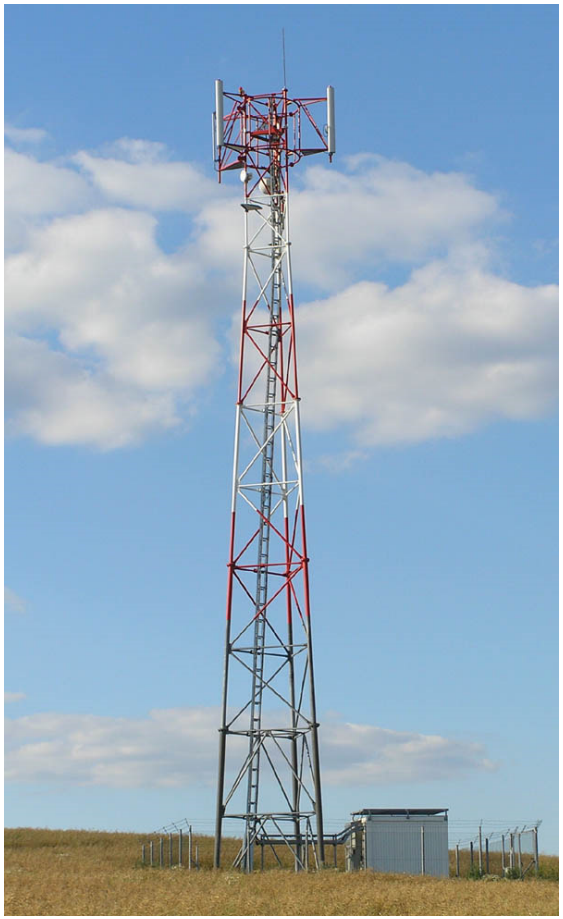
Mobile phones are tracking devices that reveal much about our lives. One look at our interactive map of data provided by the Green party politician Malte Spitz shows why. VON KAI BIERMANN

This profile reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life.

Common acronyms

- BTS: Base Transceiver Station
- SIM: Subscriber Identity Module
- PIN: Personal Identification Number
- PUK: Pin Unlock Key





Data available from SIM Card (1/2)

- IMSI: International Mobile Subscriber Identity
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- MSISDN: Mobile Station Integrated Services Digital Network (phone number)
- Network Information
- LND: Last Number Dialled

Data available from SIM Card (2/2)

- ADN: Abbreviated Dialled Numbers (Phonebook)
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Centre SMS Service Centre Info, GPRS Service Centre Info
- Location Information: The GSM channel (BCCH: Broadcast Control Channel) and Location Area Code (LAC) when phone was used last.
- IMEI: International Mobile Equipment Identity (Not on SIM, but Exclusive To GSM Devices)

Data available from mobile device (1/2)

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers

Data available from mobile device (2/2)

- Photos and Video (also stored on external flash)
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (Serial Number)
- Emails, memos, calendars, documents, etc. from PDAs
- With Smartphones – GPS Info, Social Networking Data

Android devices

- What Can Be Pulled from the Device
  - Logical Tools Acquiring Call Logs, Pics, Phonebooks
  - SIMs on many Androids Providing Last Numbers Dialled and SMS messages
  - Physical Access improving. Practitioners Rooting Device to Obtain More Data – Parsing Required
  - Most actively pursued device by mobile forensic tool players.

iPhone and iPad

- What Can Be Pulled from the Device
  - Focus Today is Getting Image of iPhone and Analysing for Data
  - Logical Tools Getting Contacts, Call logs, SMS, MMS, Pics – Much more
  - Facebook Contacts, Skype, YouTube data
  - Myspace Username and Passwords
  - Location from GPS, Cell Towers and Wi-Fi networks

Blackberry

- What Can Be Pulled from the Device
  - Most Difficult of Smartphone Devices To Pull Data
  - Limited Deleted Data acquired
  - A Handset PIN locked Device All But Impossible To Access
  - Common practice is to Get IPD Back-Up File and Analyse it. (IPD: Interactive Pager Back-up)
  - Call Logs, SMS, Pictures, Phonebook, Email, Location info from IPD Back-up file.

Example scenarios

- Ability to access the mobile phone
  - No access, temporary access, seized
- Type of access to the mobile phone
  - Passive, invasive, ability to replace parts
- Knowledge of the mobile phone keys
  - None, PIN, PUK, etc…
- State of the mobile phone
  - Functional, still powered-on, dysfunctional

BIRMINGHAM CITY University

Example scenario 1

- Ability to access the mobile phone
  - No access, **temporary access, seized**
- Type of access to the mobile phone
  - **Passive**, invasive, ability to replace parts
- Knowledge of the mobile phone keys
  - None, **PIN**, PUK, etc…
- State of the mobile phone
  - **Functional**, still powered-on, dysfunctional

BIRMINGHAM CITY University

Example scenario 2

- Ability to access the mobile phone
  - No access, temporary access, **seized**
- Type of access to the mobile phone
  - Passive, **invasive**, ability to replace parts
- Knowledge of the mobile phone keys
  - **None**, PIN, PUK, etc…
- State of the mobile phone
  - Functional, still powered-on, **dysfunctional**

BIRMINGHAM CITY University

Example scenario 3

- Ability to access the mobile phone
  - **No access**, temporary access, seized
- Type of access to the mobile phone
  - Passive, invasive, ability to replace parts
- Knowledge of the mobile phone keys
  - **None**, PIN, PUK, etc…
- State of the mobile phone
  - Functional, still powered-on, dysfunctional

Example scenario 4

- Ability to access the mobile phone
  - No access, **temporary access**, seized
- Type of access to the mobile phone
  - **Passive**, invasive, ability to replace parts
- Knowledge of the mobile phone keys
  - **None**, PIN, PUK, etc…
- State of the mobile phone
  - Functional, **still powered-on**, dysfunctional

BIRMINGHAM CITY University

Summary

- Mobile device forensic analysis has a broader scope than computer forensics.
- Forensic investigations already have a significant proportion for data captured from mobile devices.
- This proportion is going to further increase with Smart-* mobile systems.
- Convergence and standardisation of mobile device interfaces will only facilitate data extraction task.