Mobiltelefoner som bevis i brottsmål

Thomas Renman – Micro Systemation AB
thomas.renman@msab.com

Agenda – 22 maj

- Micro Systemation – vad gör vi?
- XRY video
- Mobiltelefoner som bevis i brottsmål
- Vad kan man hitta i en mobiltelefon?
- Mobiltelefonens olika lagrings enheter
- Hur får man ut informationen?

Micro Systemation AB

- Grundades 1984
- Fokus på kriminaltekniska verktyg för mobiltelefoner
- Publikt bolag, noterade på NGM börsen sedan 1999

XRY Korta fakta

- Produktutvecklingen av .XRY började 2003
- Första leveransen september 2003
- Version 2 lanserades november 2004
- Version 3 lanserades hösten 2006
- Support för 400 telefon modeller från 12 tillverkare
- Används i mer än 40 länder
- England och Holland största marknaderna

XRY Video

- C:\XRY Video\XRY Video Presentation\VIDEO_TS\VTS_01_1.VOB

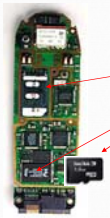
Mobiltelefoner som bevis i brottsmål


MORGAN'S SHOCK RETURN FOR ITALY
No place for Alfie in starting XV
Western Mail
'Cheating husband arranged for lover to murder his wife'

Exempel på vad kan man hitta i en mobiltelefon

- Samtalslistor
- SMS
- Kontakter
- Bilder
- Videos
- E-mail
- GPS data

Inside a Mobile Phone



- Data can be stored in 3 primary locations
  - Handset
  - SIM
  - Memory card (optional)
- Duplication may occur between these
- Handset sometimes referred to as:
  - "Mobile Station" (MS) in GSM
  - "User Equipment" (UE) in 3G

SIM Cards

Subscriber Identity Module (SIM)

- A "smart card" containing:
  - CPU
  - RAM
  - ROM
  - EEPROM
  - I/O circuits
- Stores:
  - Card identity (ICCID)
  - Subscriber identity (IMSI)
  - User data
- Defined by international standards (ETSI)
  European Telecommunications Standards Institute

Integrated Circuit Card Identifier

- ICCID uniquely identifies the card
  - 19 or 20 digits in length
  - Always stored digitally in the card
  - Normally printed on the outside (may be abbreviated)
  - Can determine issuing service provider & country from ICCID

International Mobile Subscriber Identity

- IMSI uniquely identifies a subscriber
  - Always stored digitally on the card
  - Seldom seen by, or known to, the owner
  - 15 digits in length
  - Can also determine the issuing service provider & country from the IMSI

Mobile Country Code (MCC) Mobile Network Code (MNC)

530016604508179 8

New Zealand Vodafone NZ

Universal Subscriber Identity Module

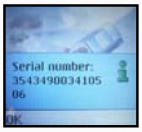
- USIM is a 3G SIM card
- Differences include:
  - Greater storage capacity
  - Enhanced phone book (e.g. nickname, email etc.)
- But same physical shape & size
  - May not be able to visually identify as a USIM
- Combination (hybrid) cards exist

Handset

International Mobile Equipment Identifier

- 15 digits in length
- Stored digitally in the handset
- Printed on a sticker under the battery
- Can determine make & model from IMEI

The two versions *should* match…



Type *#06#

Mobile Phone Memory

- Handsets contain different memory chips for data storage
  - Operating system
  - User data

- Few standards/rules govern:
  - What should be stored (except IMEI)
  - Where/how it should be stored
  - How/when it should be deleted (except call registers on SIM swap)

Mobile Phone Memory

- Contents of memory will change constantly
  - Power on/power off
  - User interaction
  - Interaction with network
- Memory provided for user data may be
  - Pre-allocated
    - e.g. Nokia 6220 limited to 20 dialled calls, 300 contacts etc.
  - Shared
    - e.g. Nokia 6630 has 10MB "shared memory"

Operating Systems

- Operating system is the manufacturer's software which makes the phone work
- Most handsets run proprietary o/s software
  - Different between different makes and models
- High-end "smartphones" may run:

Symbian OS

Windows Mobile

Palm

Connection Interfaces

- Cable
  - Fast, secure, quite reliable
- Infra-red
  - Slower, quite secure, less reliable
  - Not all data may be retrieved
- Bluetooth
  - Quite fast, less secure, less reliable, more intrusive

Bluetooth®

Memory Cards

Memory Cards

- Increasingly common in new handsets
- Different physical "form factors" exist
  - e.g. MMC, microSD, MemoryStick Duo etc.
- 4GB cards currently available (Jan '07)
- PC-compatible FAT filesystem widely adopted
- May contain pictures, movies, MP3.....or any file at all!
- Deleted data retrievable with established computer forensic techniques

Handset Extraction

Logical Extraction

- Extraction software asks handset what data is available
- Handset may or may not provide data
  - Will not provide deleted data
- Different protocols are used for:
  - Different handsets
  - Different data types

Protocols Used in Logical Extractions

- AT
  - Identification, basic information for most GSM models.
- OBEX ("OBject EXchange")
  - Pictures, audio, video
  - Different flavours for different makes and models
- IrMC, SyncML
  - OBEX based protocols. Phone book, calendar, notes
- FBUS
  - Nokia's binary protocol. Differences for almost each model.

Results from Logical Extractions

- The following data may be retrievable
  - Phonebook/contacts
  - Call registers (dialled, missed, received)
  - SMS
  - MMS
  - Photos
  - Movies
  - Audio files (ringtones, MP3, recordings)
  - Calendar / appointments / tasks / notes
  - Games & other software
  - And more…

Physical Extraction

- Physical extraction involves either
  - Removing chips from circuit board & "dumping" contents (destructive)
  - Via a data cable (e.g. service ports on many Nokias)
- Data is supplied in a "raw" form
  - Interpretation requires time & specialist knowledge
  - Provides a lot of data including deleted handset information

Frågor?