IMF 2009
Stuttgart, Germany

Complete Mobile Phones Forensic Examination:
Why we need both Logical & Physical Extractions

Martin Westman - Micro Systemation

MICRO SYSTEMATION

Agenda

- Our Backgrounds
- Live Demo of physical and logical benefits
- Questions and Discussion
- Extreme Hex-Dumping (or Hex-Jumping)

MICRO SYSTEMATION

Our background

- Martin Westman
  - Product Specialist
  - Collecting information / req. from LE
  - User Trainer
- Micro Systemation
  - Long experience from Mobile Forensics
  - Work Globally
  - User Training

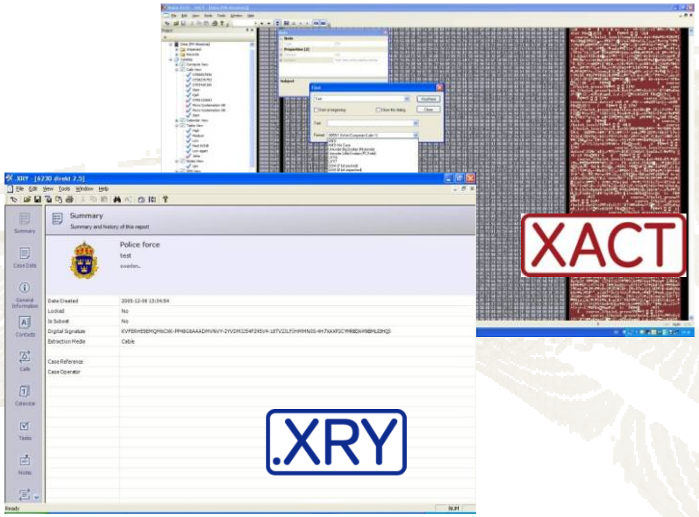
Facts & trends

- Study from Europol and European Commission: in over 70% of solved criminal cases in Europe involved phone forensic, also confirmed in the US by DC3's Jim Christy
- In UK / Sweden / Germany /France its over 90%

Different solutions for Mobile Forensics

paraben
forensic tools

Forensic
Telecommunications
Services
FTS



Summary
Summary and history of this report

Police force
test
sweden..

Date Created 2005-12-08 13:34:54
Locked No
Is Subset No
Digital Signature KVFERHE9EMQP6CXK-PP4BG8AAADMVNVY-2YVDM3254F2X5V4-18TV2ILFIHMMN0S-4H7XAXP3CYMRBDW9BML2BHQS
Extraction Media Cable

Case Reference
Case Operator

MICRO SYSTEMATION

Logical and physical extractions, two ways of extracting data

logic

physical

What to expect of a logical extraction tool today:

- Quick, easy to use and reliable
- 100% forensic secure
- Extracts ”all” data
  contacts, calls, calendar, SMS, photos etc
- Reports in local language

What Can a Logical Extraction Retrieve?

LIVE	Live SIM data can be retrieved	Live handset data can be retrieved
DELETED	Only deleted SMS can be retrieved (using card reader)	Deleted handset data cannot be retrieved

Demo Logical Extraction Nokia

MICRO SYSTEMATION

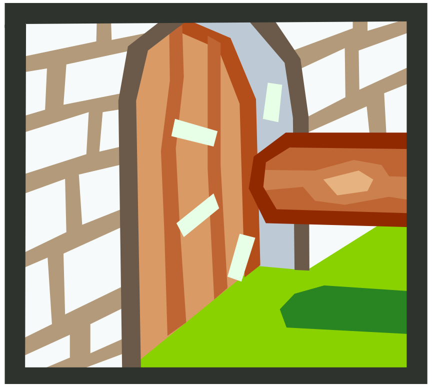
The Physical alternative

- Creates a “complete” Memory Image
- Extracts even
  - deleted data
  - system information
  - Mobile Network Provider information
  - Previous IMSI(s)
- Retrieve data from devices where no SIM is present
  - Bypass (and retrieve) handset security codes
- Memory card analysis
- Automatic decoding of binary data?
- View the data in it’s raw Hex-format
- Export / Import functionality

How to do a Physical Extraction? (“hex dump”)

✓Physical extraction involves either

- –Cable connection and specific software
- –Removing chips from circuit board & “dumping” contents (sometimes not repeatable)



✓Data is supplied in a “raw” form

- –Interpretation requires time & specialist knowledge
- –Provides a lot of data including deleted handset information

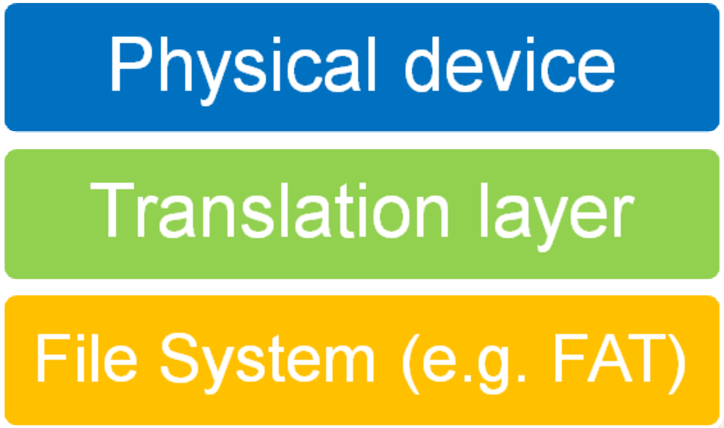
```
DD 33 99 C9 77 22 D9 BF 65 02
82 68 16 D5 AF 2B D3 E5 D4 7B
4D 02 0A 21 8B B4 18 14 0D 2A
DC 19 F0 DC DB E0 EE DC AA 73
6B D9 4C 3D C3 27 69 5F 36 6E
96 B1 37 33 26 4D 56 B8 73 C0
29 DE EE EC 8C B7 9F A6 8D 6C
```

Disadvantages of Memory Dump Approach

- Harder to retrieve data
- More data to interpret
- Harder to interpret data
- Less devices supported

Translation Layers

- ✓Flash memory has a limited number of write/re-write operations before failure
- ✓Sensible NOT to always write data to the same physical locations
- ✓Flash memory uses “wear levelling” algorithms to spread usage across the device (thereby extending lifetime)

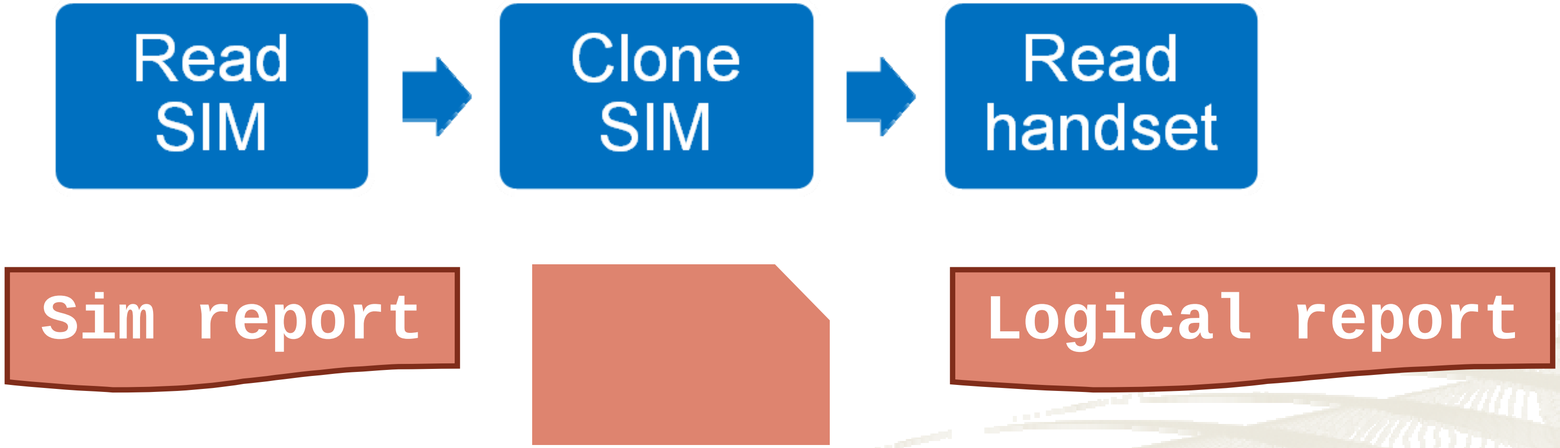


Physical device

Translation layer

File System (e.g. FAT)

The traditional workflow of logical extraction Processes



Read SIM

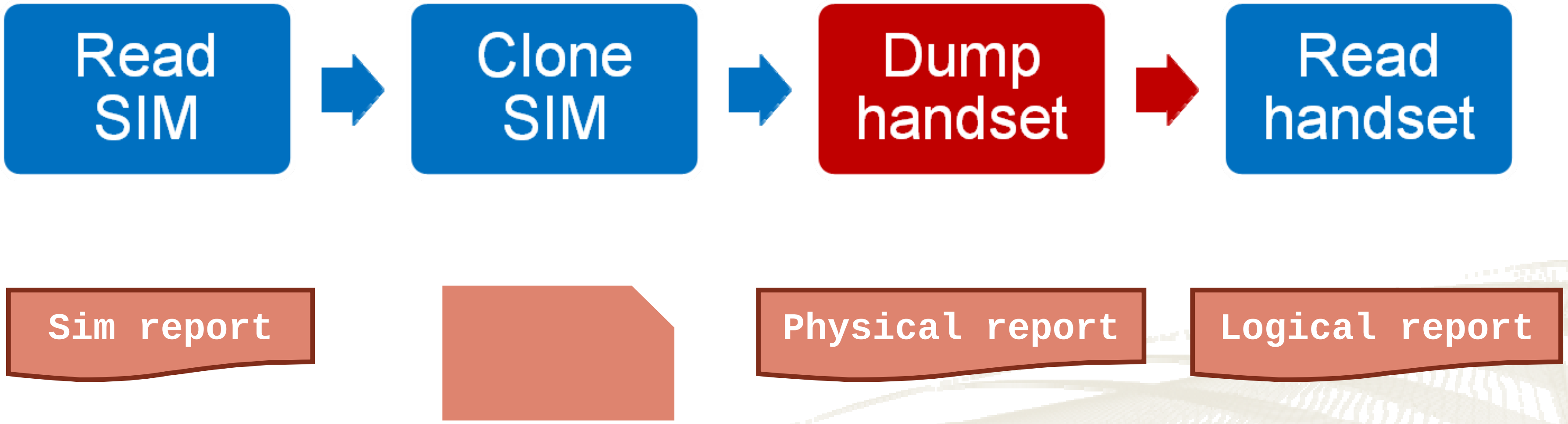
Clone SIM

Read handset

Sim report

Logical report

Integrating Hex-dumping into Traditional Processes



Read SIM

Clone SIM

Dump handset

Read handset

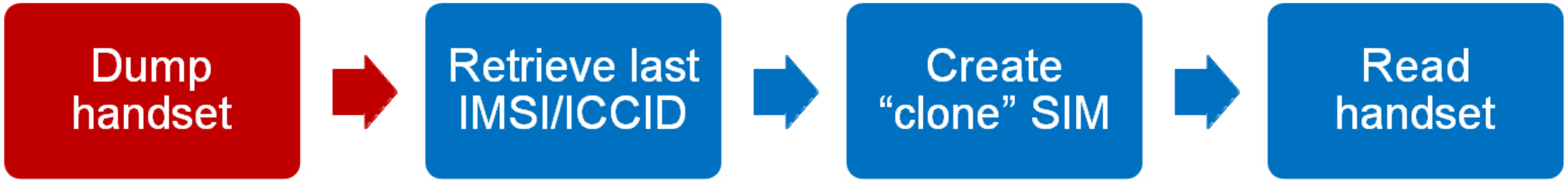
Sim report

Physical report

Logical report

Targeted Memory Dumping 1

No SIM Present – IMSI/ICCID Required for Clone SIM



Dump handset

Retrieve last IMSI/ICCID

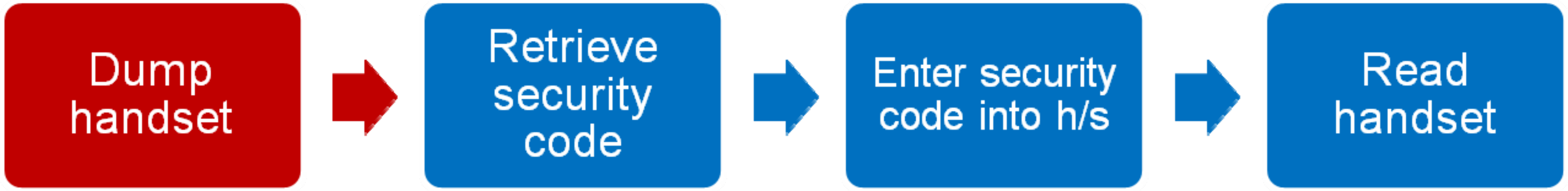
Create “clone” SIM

Read handset

Handset can be read with no loss of call registers and no incoming calls/messages

Targeted Memory Dumping 2

Handset Security Code Locked



Memory dump is the enabler. It “kick starts” the logical extraction by providing vital information

Demo Hex-Dumping Nokia and Motorola

MICRO SYSTEMATION

Extreme Ironing, What’s up with that?

- You take an un-cool thing like ironing
- And do it on a really cool place

- Soo....
- What if you took a really COOL thing and did it on a cool place?

Extreme HEX-Dumping

SIM cloner tool / Faradays Cage

➢ 3 scenarios for using SIM id-Cloner / FC when extracting phones:

- Isolate the phone from mobile network
- Phone without SIM-Card
- PIN-code protected phones

MICRO SYSTEMATION

Demo Motorola

Logical Acquisitions & Memory Cards

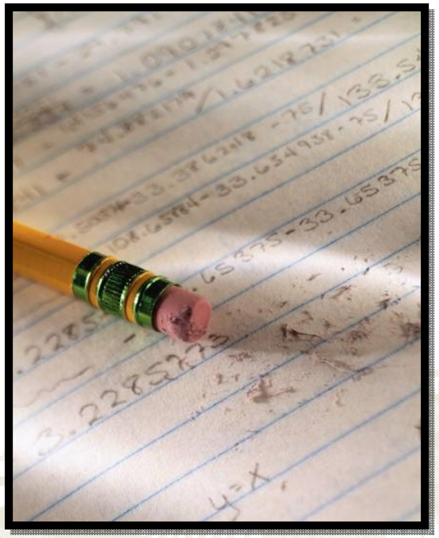
- ✓Logical tools can recover live data from memory cards within handsets
- ✓The phone never provides deleted files during a logical acquisition
- ✓Memory card needs to be accessed directly to retrieve deleted data
- ✓How can we pullback deleted files?

Combined Reports

- ✓Wouldn’t it be nice to be able to combine the reports?
- ✓You can add an XACT extraction to an .XRY report
- ✓The added report will show up as an extra tab

File Deletion in FAT

✓Most phones will have a FAT based file system internally, and is the unofficial standard on memory cards in mobile phones.



✓When a file is deleted from a FAT partition:

- The file's directory entry is changed to show that the file is no longer needed
  - 1st character of filename is replaced with a 'marker'
- The file data itself is left unchanged

Hashing

✓Hashing the same data with the same algorithm always gives the same result

- If the data changes, the hash will be different (i.e. NOT applicable in hex-dumping, only for individual files)

✓Uses of hashing in digital forensics

- To prove that a unit of data has not changed
- To identify files that have been seen before (“hash libraries”)
  - e.g. known indecent pictures
  - e.g. operating system files

Summary

- Using both logical and physical extractions gives the investigator a better view.
- Physical tools can successfully be used to enable phones for logical extraction.
- Decoding of Physical data is hard, there are no standards in mobile phones.

THANK YOU for listening!

Martin Westman

Product Specialist

Micro Systemation Inc
martin.westman@msab.com

+46 709 189 585

MICRO SYSTEMATION

IMF 2009
Stuttgart, Germany

Complete Mobile Phones Forensic Examination:
Why we need both Logical & Physical Extractions

Martin Westman - Micro Systemation AB

MICRO SYSTEMATION