10 Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics

By

Ronald van der Knijff

Presented At

The Digital Forensic Research Conference

DFRWS 2007 USA Pittsburgh, PA (Aug 13th - 15th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

10 Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics

Ronald van der Knijff
Netherlands Forensic Institute
knijff@holmes.nl

Justitie

Outline

1. Small Scale Digital Devices are in the majority
2. On the long term everything is small scale
3. SSDDs have great forensic potential
4. Anti-forensics is more difficult
5. It lags behind other digital forensics fields
6. It's uncultivated so easy to score on

   Forensic Data Recovery from Flash Memory
7. It's so diverse, it needs more people
8. You like new gadgets
9. You need to do something different
10. We just need you !

Justitie

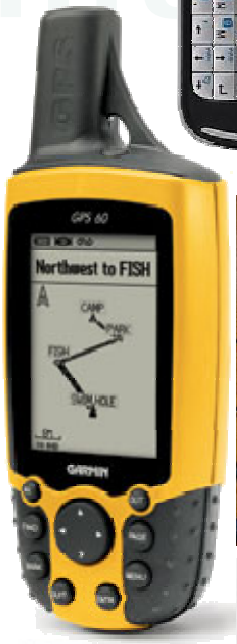
Small Scale Digital Devices

- Cyber Forensic Hardware Ontology:
  (www.dfrws.org/2006/proceedings/5-Brinson.pdf)
  - Large Scale Digital Devices
  - Small Scale Digital Devices (SSDD)
  - Computers
  - Storage Devices
  - Obscure Devices
- SSDD Ontology (www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf
  - Personal Digital Assistants
  - Cellular Telephones
  - Audio / Video Devices
  - Gaming Devices
  - Embedded Chip Devices

Embedded Systems

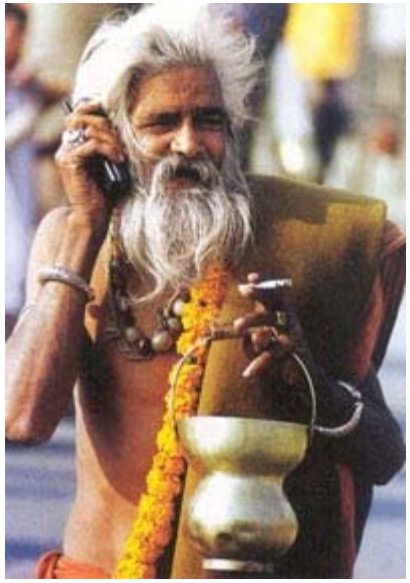
Justitie

Embedded Systems



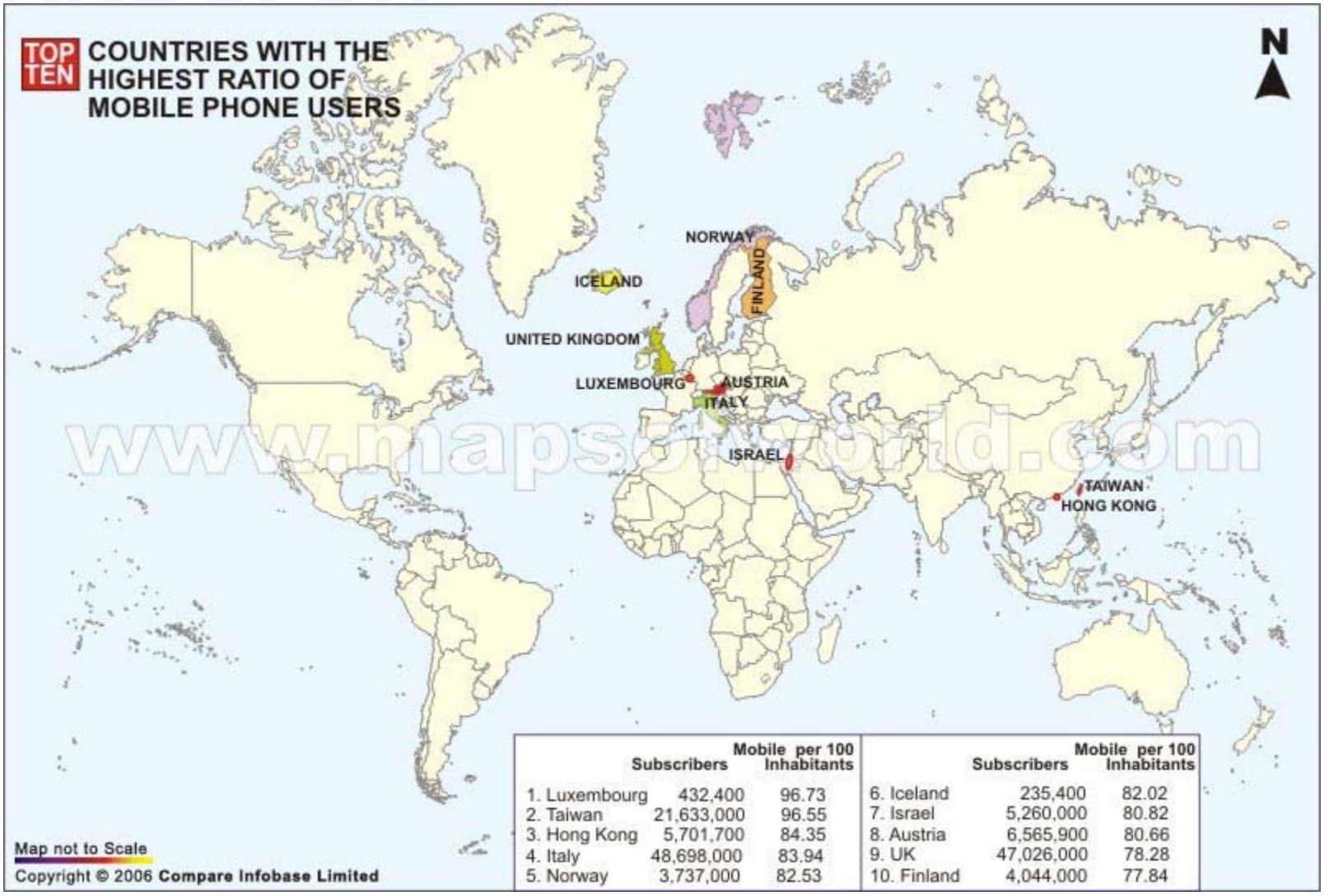
Small Scale Digital Devices are in the majority

- Netherlands 2006: 84% of all households have access to PC, 80% to Internet
- 2006: 30 countries passed 100% mobile phone penetration (US: 72%)
- Netherlands 2007: 107 mobile phone subscriptions per 100 inhabitants ⇒ >17,514,889 subscriptions
- Dutch inhabitants statistics:
  - 67% always wear mobile phone
  - 51% never switch it off
  - 9% take phone call during sex
  - most popular functions besides calling: sms, weak-up-timer, camera
- Number of camera phones will reach 1 billion this year
- One third of the world population will own a camera phone by 2011
- Within 2 years 60% of sold notebooks is predicted to have flash storage instead of magnetic disks (24 million notebooks Q4 2009)



Justitie

Small Scale Digital Devices are in the majority



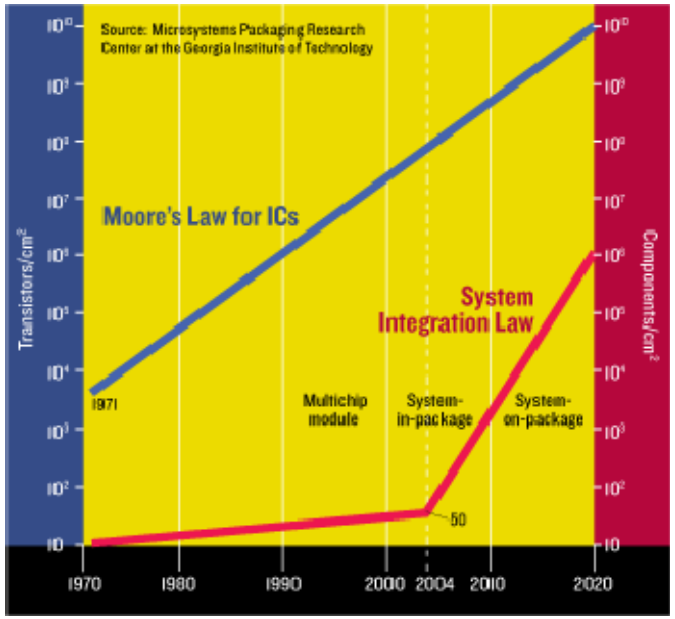
	Subscribers	Mobile per 100 Inhabitants
1. Luxembourg	432,400	96.73
2. Taiwan	21,633,000	96.55
3. Hong Kong	5,701,700	84.35
4. Italy	48,698,000	83.94
5. Norway	3,737,000	82.53

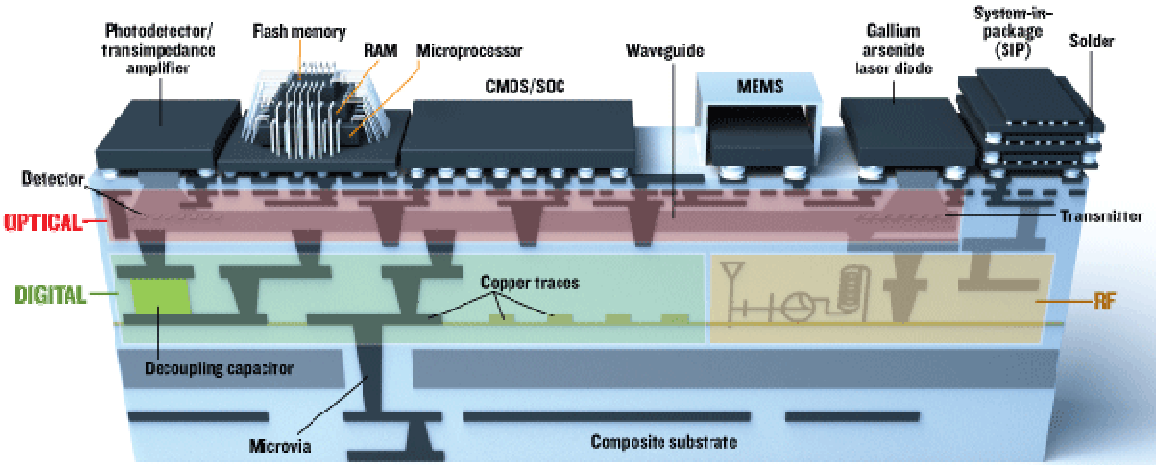
	Subscribers	Mobile per 100 Inhabitants
6. Iceland	235,400	82.02
7. Israel	5,260,000	80.82
8. Austria	6,565,900	80.66
9. UK	47,026,000	78.28
10. Finland	4,044,000	77.84

Justitie

On the long term everything is small scale

- Moore's Law Meets Its Match, Rao R. Tummala (www.spectrum.ieee.org/jun06/3649):



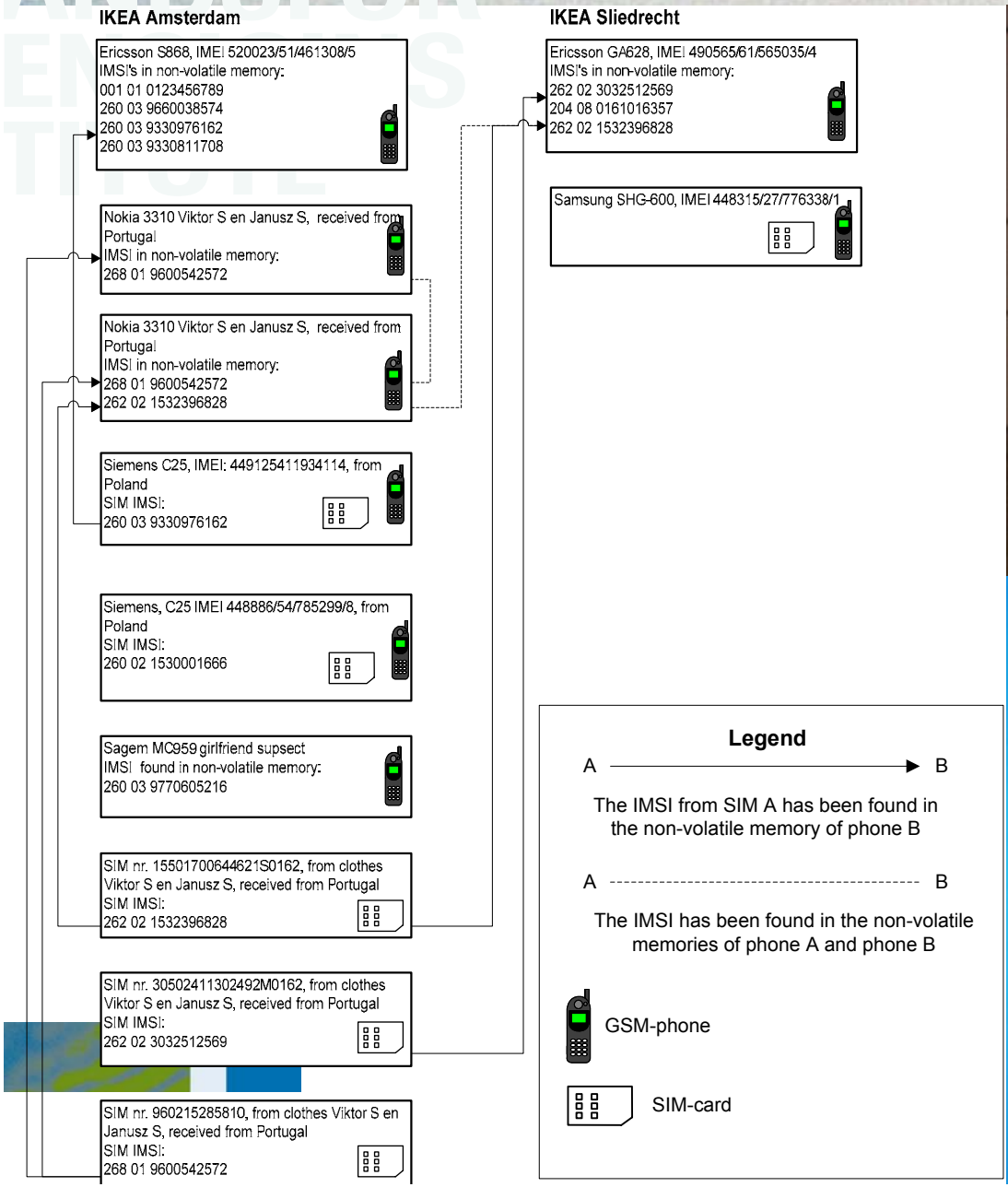


SSDD forensic potential

- Most serious crimes are aimed at persons and committed by persons ⇒ personal related data is most interesting
- Most criminals are not committing a crime at their home ⇒ geographical related data is interesting
- SSDD's are often very personal related, portable and increasingly leave geographical related traces
- Metcalfe's Law: The value of a network grows in proportion to the square of the number of users
- SSDD most popular memory for user data is flash EEPROM:
  - Flash is solid state memory
  - Flash is non-volatile
  - Flash can only be erased in blocks
- Flash has more forensic potential then magnetic or optical storage technologies

Justitie

SSDD forensic potential



Forensic Potential – Phone Example Case

www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

- Mobile Phone Samsung SGH-D500
  - Multi-Chip Package MEMORY
    - 32 MByte NOR Flash
    - 64 MByte NAND Flash
    - 16 MByte RAM
  - MMC interface for external cards
- NAND flash data analysis
  - FAT16 file system on top of a flash translation layer
  - Not all flash blocks are part of the FAT16 FS
  - Found 83 versions of FAT part and 1464 versions of the directory '\multimedia\VIDEOS\video clips'
  - Fragments of erased video were found in flash data outside of FAT FS

Justitie

Anti-forensics is more difficult

- SSDDs are more closed then ‘normal computers’
- Users are not aware of what data is stored
  - Mobile phone call detail records
  - Chipcard transaction loggings
  - Embedded software execution residues
- Users can’t access all data
  - No low-level interfaces are available
- Because of the big variety and the lack of standards less ‘script kiddy tools’ exist
- But: be careful for data loss and data contamination: RAM, online devices (phone, PDA), data generating sensors (GPS) …

SSDD forensics lags behind other digital forensics fields Tools

- Before 1995: no forensic SSDD applications known
- 1995: ZERT — NFI LE-only tool for cracking PDA passwords
- 1998: Cards4Labs — NFI LE-only tool for reading SIM cards
- 2000: TULP — NFI LE-only tool for reading phones
- pdd, Encase, PDA Seizure — First commercial tools for forensic examination of PDA's
- 2004: .XRY — First major commercial tool for forensic examination of mobile phones (logical data extraction)
- 2004: TULP2G — NFI open source forensic framework for SSDD data acquisition and decoding
- MobileEdit! Forensic, Oxygen Phone Manager Forensic, SIMCon, Device Seizure …
- 2006: FTS Hex — First forensic tool for low level examination of mobile phones (physical data extraction)
- 2007: Neutrino — Mobile phone examination integrated into Encase

Justitie

SSDD forensics lags behind other digital forensics fields Procedures

- 2005: NIST — Guidelines on PDA Forensics
  http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf
- 2005: NIST — PDA Forensics Tools: An Overview and Analysis
  http://www.csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf
- 2005: NIST — Cell Phone Forensic Tools: An Overview and Analysis
  http://csrc.nist.gov/publications/nistir/nistir-7387.pdf
- 2006: Interpol — Good Practice Guide for Mobile Phone Seizure & Examination
  http://www.holmes.nl/MPF/Principles.doc
  http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm
- 2007: NIST - Guidelines on Cell Phone Forensics
  http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

Justitie

Forensic Data Recovery from Flash Memory

- Flash technology basics
- Tree possible data acquisition techniques
  - Flasher Tools
  - JTAG
  - Physical Extraction
- Translate flash data to file system level
- Specific flash artefacts

- Flash technology basics: storing electrical charge into the floating gate of a transistor
  - Data retention: 10-100 years
  - Basis data operations
    - Erase (resetting a block of cells to '1' state)
    - Program (setting an individual cell to '0' state)
  - Cells 'wear out' after 10^4-10^6 erase cycles
  - Wear levelling: methods to spread the erasing of blocks as evenly as possible

Justitie

Forensic Data Recovery from Flash Memory
Data Acquisition Techniques: Flasher Tools

- Using external interface to copy data from flash to target system
- SSDD's don't have a common external interface
- Mobile phones flasher tools mainly originate from:
  - Manufacturers or service centers for debugging/repair/upgrade
  - Hackers for checking and changing device functionality

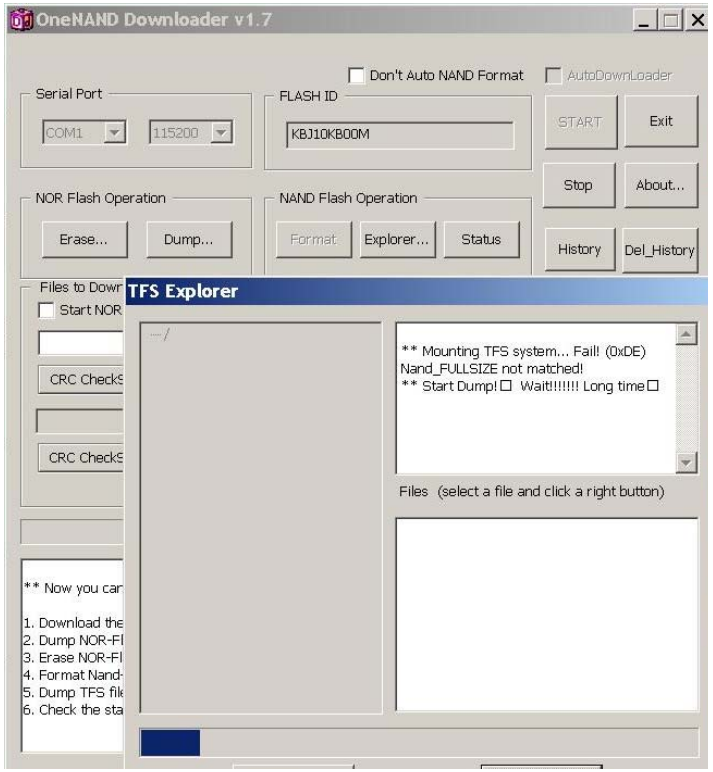
☺ Easy to connect and use

☹ Not all tools make a complete copy

☹ Some tools change data

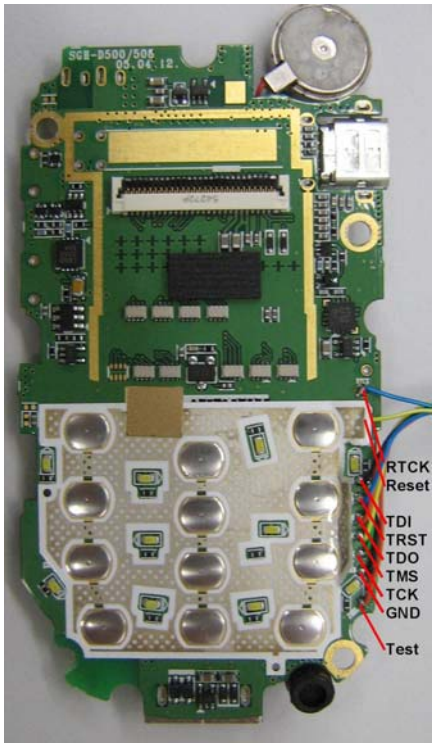
☹ Tools often have dangerous options

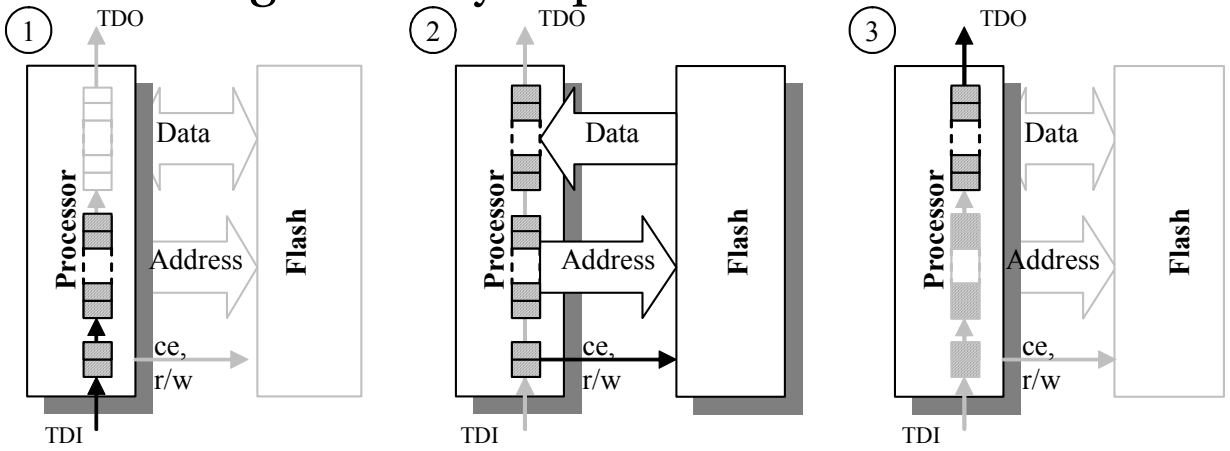
☹ You need a reference phone to practice



Forensic Data Recovery from Flash Memory
Data Acquisition Techniques: JTAG

- JTAG test access port is normally used for testing and debugging
- Can also be used for making memory copies:



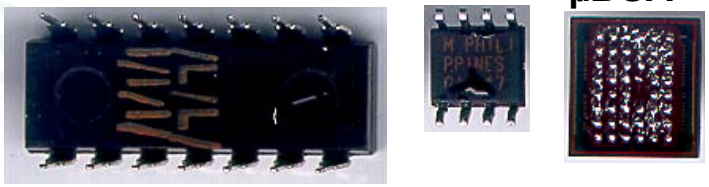


☺ No de-soldering of flash memory chips
☺ A complete forensic image can be produced
☺ The risk of changing data is minimized
☹ Can be slow
☹ JTAG test access point can be difficult to find
☹ Not all embedded systems are JTAG enabled

Justitie

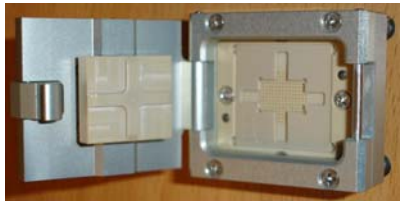
Forensic Data Recovery from Flash Memory
Data Acquisition Techniques: Physical Extraction

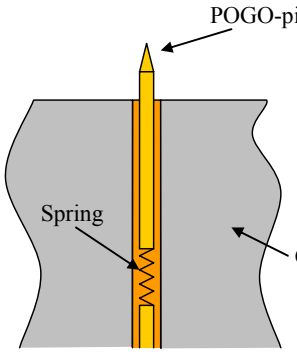
Chip generations:



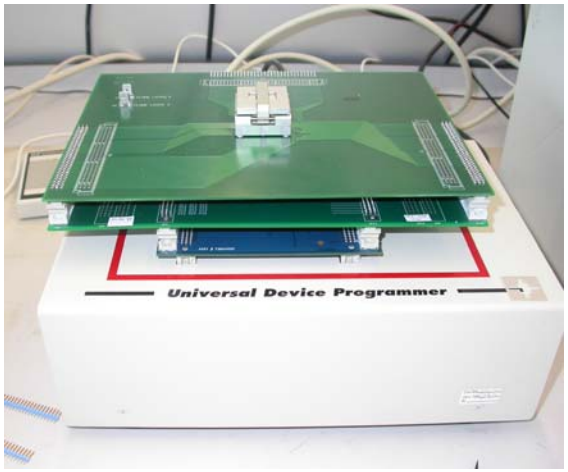
1) Removal of µBGA chip with rework station

2) Cleaning and connecting to Universal BGA Test Socket



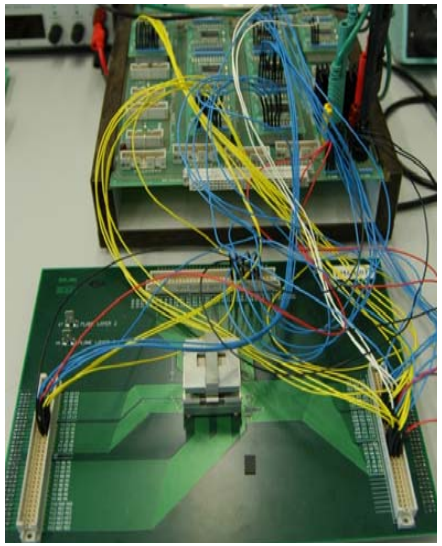


3a) Data extraction with commercial device programmer, or with…



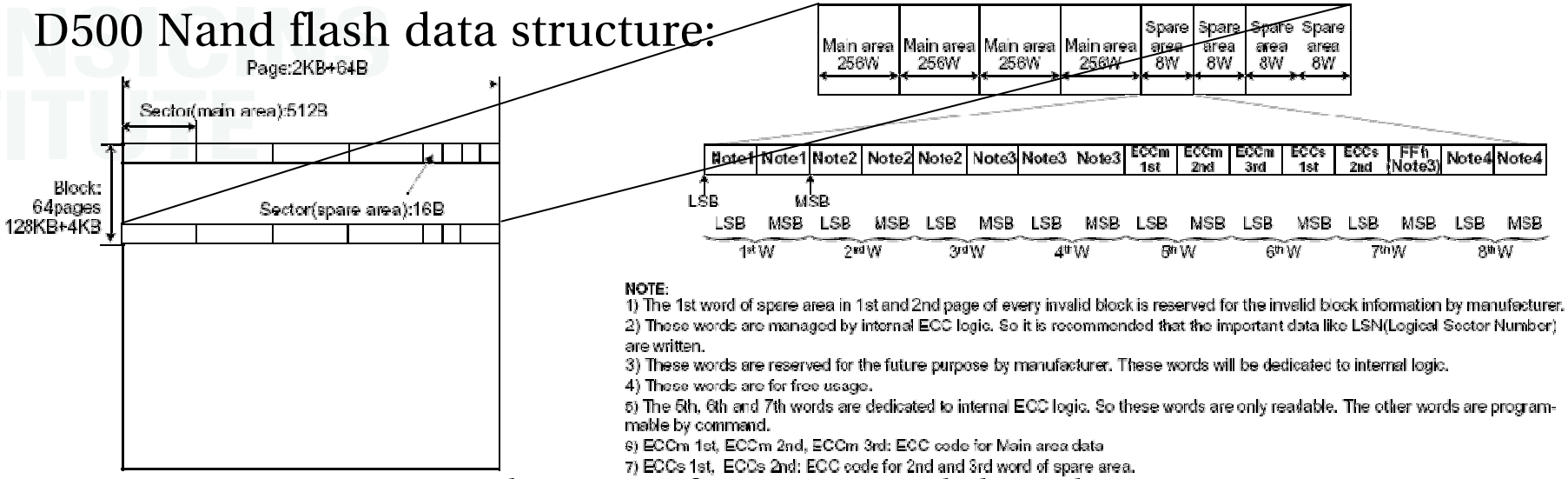
3b) NFI memory toolkit

- ☺ Device does not need to be functional
- ☺ Copy without any changes
- ☹ Expensive
- ☹ Small risk for total data destruction



Forensic Data Recovery from Flash Memory
Translate flash data to file system level

- D500 Nand flash data structure:



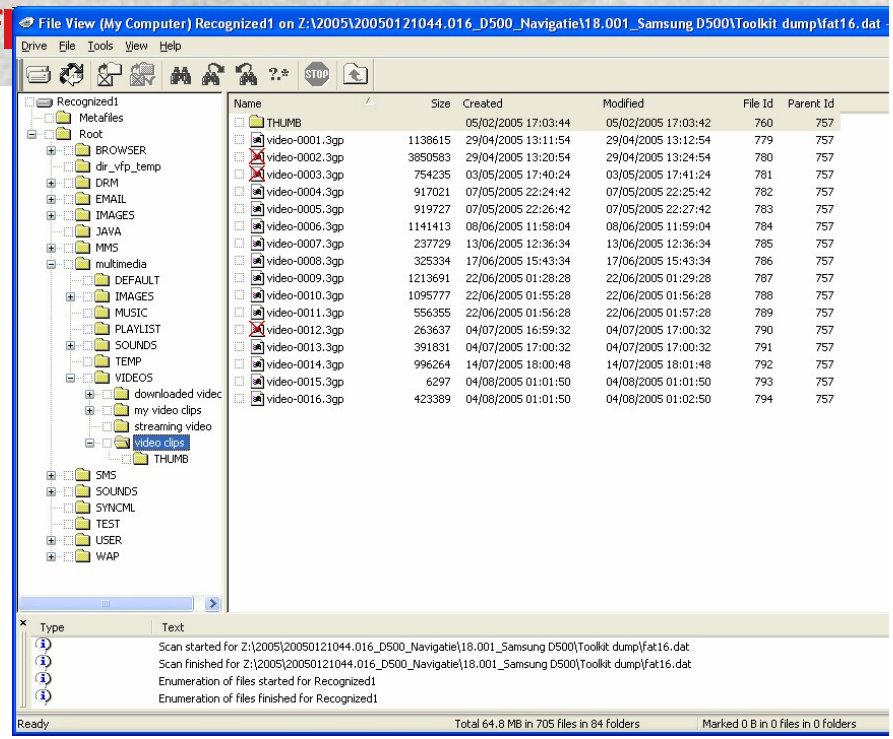
NOTE:
1) The 1st word of spare area in 1st and 2nd page of every invalid block is reserved for the invalid block information by manufacturer.
2) These words are managed by internal ECC logic. So it is recommended that the important data like LSN(Logical Sector Number) are written.
3) These words are reserved for the future purpose by manufacturer. These words will be dedicated to internal logic.
4) These words are for free usage.
5) The 5th, 6th and 7th words are dedicated to internal ECC logic. So these words are only readable. The other words are programmable by command.
6) ECCm 1st, ECCm 2nd, ECCm 3rd: ECC code for Main area data
7) ECCs 1st, ECCs 2nd: ECC code for 2nd and 3rd word of spare area.

- From experiments with NFI reference model and TSK:
  - Each block contains a Block Version (BV)
  - Each spare area contains a Logical Sector Number (LSN)
  - Identical LSN's exist
  - For physical sectors with identical LSN's the physical sector with the highest physical address must be used within the block with the highest BV to reconstruct the FAT16 file system
  - Heuristic to put non FAT-FS physical sectors in "most logical order"

Justitie

Forensic Data Recovery from Flash Memory
Specific fi

- D500 case: search for erased video
- R-Studio reported successful recovery but this was not correct
- Started with small files from THUMB folder
- Used TSK *fls* and *istat* tools:



`fls -o4 -f fat -r  D500_FATFS.bin` gives for "video-0003.3gp":

```
   ++++ r/r * 5901:        video-0003.3gp
```

`istat -o4 -f fat D500_FATFS.bin  5901` gives:

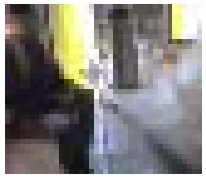
```
Directory Entry: 5901
Not Allocated
File Attributes: File
Size: 2720
Name: _IDEO-~3.3gp

Directory Entry Times:
Written:        Tue May  3 17:41:24 2005
Accessed:       Tue May  3 00:00:00 2005
Created:        Tue May  3 17:41:24 2005

Sectors:
88909 88910 88911 88912 88913 88914 88915 88916

Recovery:
File recovery not possible
```

```
ListLSN[88913]= {0x06a7c940, 0x044515b0, 0x0444e430, 0x067e0540}
ListLSN[88914]= {0x06a7cb50, 0x044517c0, 0x0444e640, 0x067e0330}
ListLSN[88915]= {0x06a7cd60, 0x044519d0, 0x0444e850, 0x067e0120}
ListLSN[88916]= {0x06a7cf70, 0x04451be0, 0x0444ea60, 0x067dff10}
ListLSN[88917]= {0x06a7d180, 0x04451df0, 0x0444ec70, 0x067dfd00}
ListLSN[88918]= {0x06a7d390, 0x0444ee80, 0x067dfaf0}
ListLSN[88919]= {0x06a7d5a0, 0x0444f090}
ListLSN[88920]= {0x06a7d7b0, 0x0444f2a0}
```



Justitie

Forensic Data Recovery from Flash Memory
MPEG4 Visual Object Plane (VOP) carving

- Goal: recovery of individual frames of deleted/corrupted MPEG4 coded video files(.3gp or .mp4 files) from memory dumps
- MPEG4 standard: **vop_start_code = B6**

```
00000000 0000 01B6 1003        0669 F727 B530 23C1 99B0 .......i.'.0#...

start_code_prefix
start_code_value 0xB6
0x1 = 0b0001
vop_coding_type
modulo_time_base
marker_bit
```

vop_coding_type coding method
00 intra-coded (I)
01 predictive-coded (P)
10 bidirectionally-predictive-coded (B)
11 sprite (S)

Search on 0x000001b6 for all VOPs

Search on 0x000001b61 for I-VOPs

Search on 0x000001b65 for P-VOPs

Search on 0x000001b69 for B-VOPs

- Run script on flash dump, preferably after sectors have been put in file system order

Justitie

- Goal: recovery of individual frames of a deleted/corrupted H.263 coded video file (.3gp or .mp4 files) from memory dumps
- H.263 standard (paragraph 5.1): Picture Start Code = 0x00008[0-3]

```
0000A378 0000 8302 0A10 36B1
0b00000000 00000000 10000011 00000010 00001010 0001000000110110101100001…
Picture Start Code
Temporal Reference "frame sequence number"
Type Information
        Static values
        Picture-Coding-Type: 0=I, 1=P
```

Forensic Data Recovery from Flash Memory
Viewing Video Fragments

- Standard players are not happy with partial or corrupted video files
- Tested some players: Quicktime, WMP, VLC, and ffplay: ffplay is most robust
- ffplay is a test viewer for the ffmpeg library (http://ffmpeg.mplayerhq.hu/index.html)
  - Very primitive GUI, undocumented key: [s] to step through individual frames
- All players are very critical on .3gp Isomedia files (because of metadata)
- Pragmatic approach to view MPEG4 carve results:
  - Search frames and save as vopdump
  - Get one reference movie “refmovie.mp4” from the same brand/type phone
  - Generate valid raw file: mp4box -raw 1 refmovie.mp4 (produces refmovie.cmp)
  - Put header from refmovie.cmp into vopdump and rename to vopdump.cmp
  - Convert vopdump.cmp to vopdump.3gp: mp4box -add vopdump.cmp vopdump.3gp
  - Play with ffshow
- H.263 frames don’t need additional header data
- Quick and dirty way to show images from video data:
  - Use carving scripts to find (only I) frames
  - Use ffmpeg to convert video file to mjpg
  - Load mjpg file in Encase and use picture search, or export jpegs from mjpg file with data carver

Wrap'up

- Small Scale Digital Device Forensics needs more attention
- Trends
  - Mobile = Portable PC = PDA + Phone + Internet + Navigation + Camera
  - Big rise in available SSDD photo, video and geographical data
  - SSDD data increasingly turns into a company security risk ⇒ more security
  - Mobile storage encryption and mobile end-to-end encryption
- Future Research
  - Flash ECC checking
  - Forensic flasher boxes
  - Flash data analysis
  - Integrating SSDD data analysis with existing computer forensic tools
  - Carving video frames and audio chunks (bit boundaries !)
  - Forensic, fault tolerant multimedia player
  - …

Justitie