



Netherlands Forensic Institute
Ministry of Security and Justice

Digital Forensics at NFI

Erica Rietveld
Manager Digital Technology
& Biometrics

Netherlands Forensic Institute

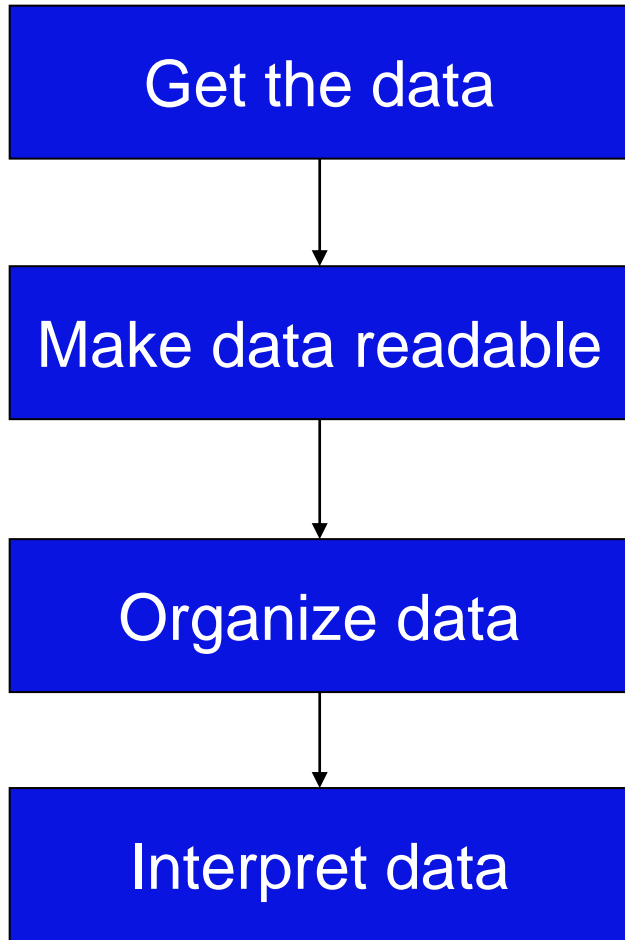
28 March 2011



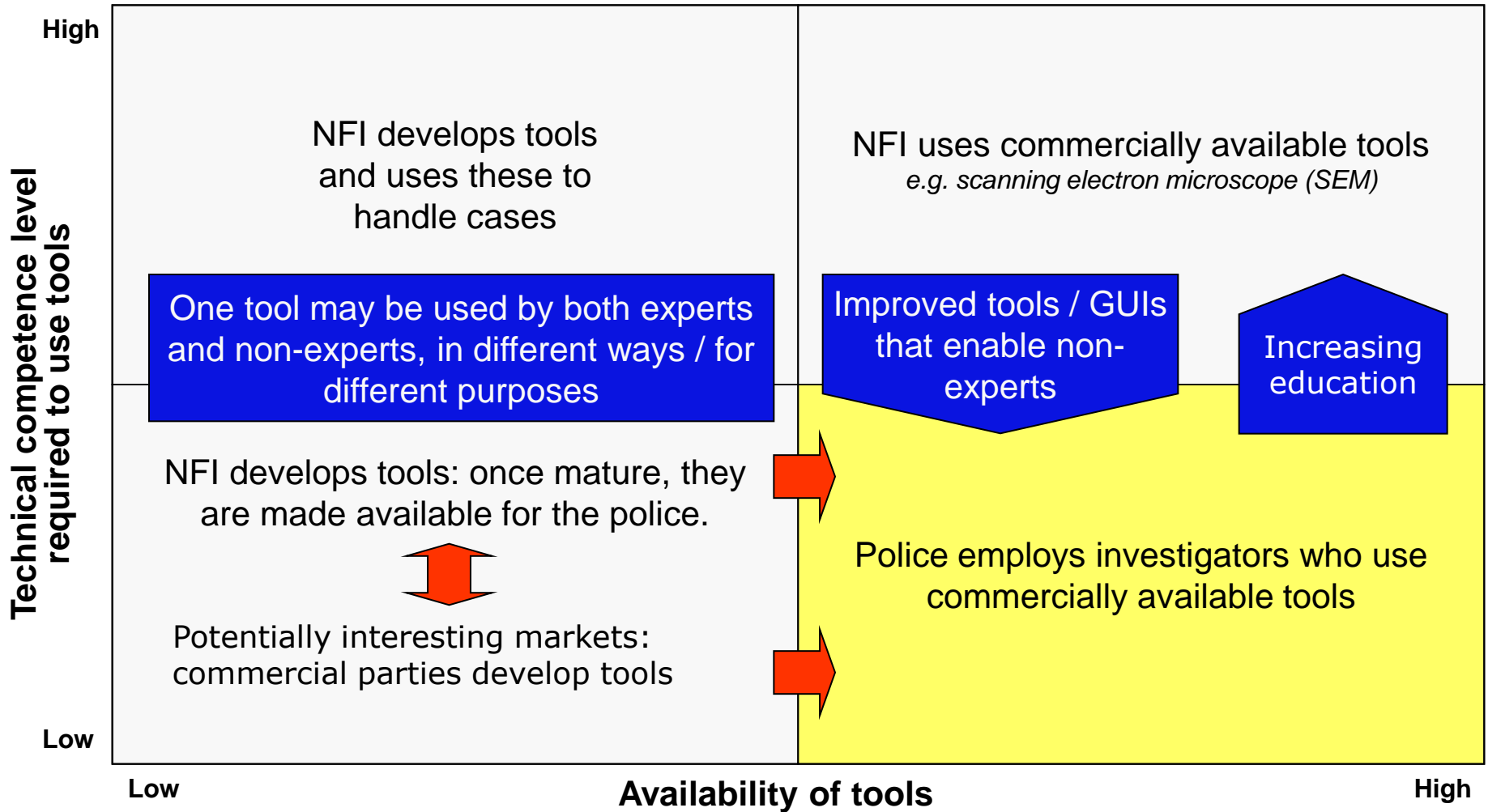
Digital forensics at NFI

Extract digital data from any damaged or working source software or hardware, and provide tailor made solutions to interpret the data in terms of digital traces in a criminal case

Focus on digital evidence



Digital evidence: tools are a prerequisite





Problem: access

- Media is damaged
- Passwords
- Encryption
- Deleted files, slack space
- Partially damaged files





Extracting data from devices

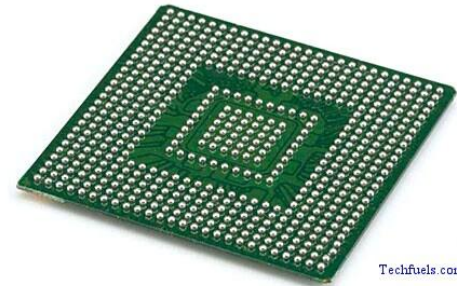
- Retrieve data from electronic devices on chip level and silicon level.
- Wide range of telephones or other electronics because generally they have the same type of memory components





Chip forensics: Memory Toolkit II

- Universal forensic solution to read memory chips
- Copy of all data in a memory chip, including information from spare areas, bad blocks etc.
- Memory chips from password locked devices can also be read
- Even memory chips from non functional target devices (damaged by heat, water or force) can be read
- No data is changed





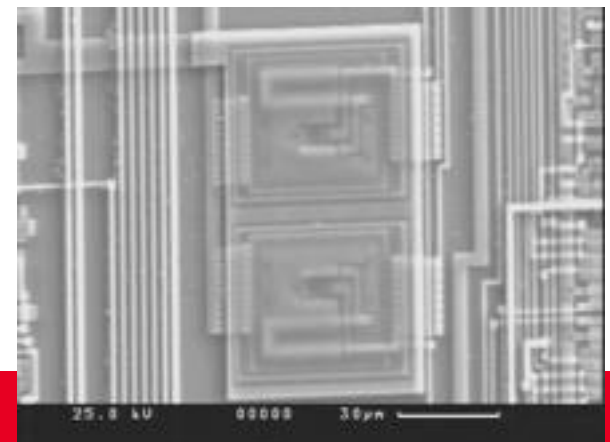
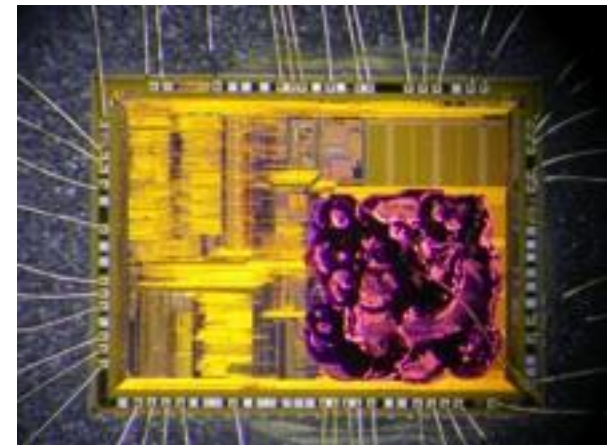
Silicon forensics

IMAM - Silicon hacking project

Invasive Memory Access Methods

- Goal: development of methods for getting access to the silicon of live chips and changing their behavior in order to readout their memory that is not accessible via the normal contacts.
- Format: a “toolbox” containing equipment and methods.
- Process: no standard process is offered, since each chip is different.

Dual
Beam
SEM





Problem: many formats, old & new, non-standard

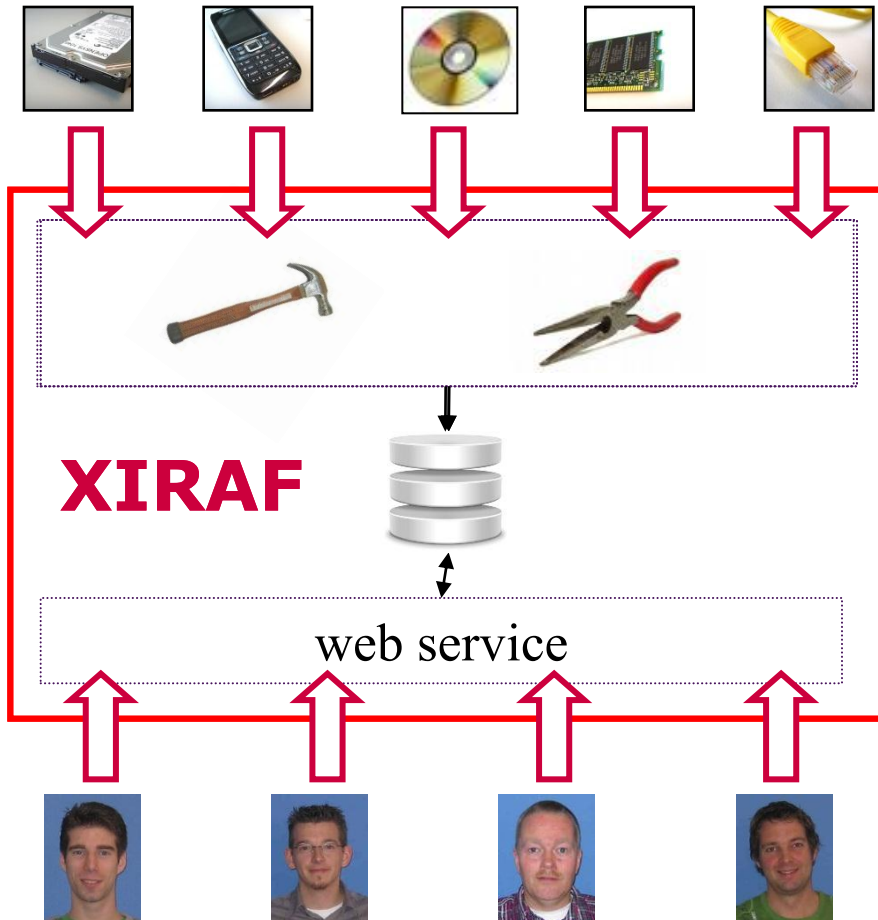
Reverse engineering: discover the technological principles of a system (e.g. software or communication protocol) through analysis of its function and operation

```
000025c0 0e 4a 5b fc 74 d6 21 a2 fb d3 5d bf 59 45 11 9a |.J[.t.!...].YE..|
000025d0 fd d6 00 28 d6 6f a1 b0 60 59 6c ce c6 d0 4c 5c |...(.o..`Yl...L\|
000025e0 61 10 8d cf 95 41 c1 3e b3 f3 62 ff 1b b0 fc dc |a....A.>..b.....|
000025f0 ea 5b fb 07 95 27 28 59 9a 05 e0 06 27 7b 2a 59 |.[...'(Y....'(*Y|
00002600 0e 43 72 1b ce 4b 1f 59 e2 ce d9 f3 86 34 5e f9 |.Cr..K.Y....4^.|
00002610 38 d1 4a 0f 06 2e 70 66 c9 49 01 00 7b ca 93 c2 |8.J...pf.I..{...|
00002620 6d 70 02 ab b6 78 90 e1 5b ca 1c 14 29 13 77 93 |mp...x..[...].w.|
00002630 9f 29 a4 d1 1f 1f 3f 20 69 29 c4 ae fd c3 01 bf |.)....? i).....|
00002640 76 c4 bd a8 cc 99 0b e3 93 74 82 b8 1e cc 2e da |v.....t.....|
00002650 64 eb 74 64 5c 6c d7 91 78 5a 58 5b 59 c5 9a 82 |d.td\l...xZX[Y...|
00002660 4d e0 2c 58 1b 5c 83 c7 7e 98 3e 37 b2 93 99 90 |M.,X.\...~.>7....|
00002670 fd 00 e0 3a 8e 4f 13 e5 1f 23 bb b5 f8 b0 a3 85 |...:0...#.....|
00002680 86 74 b9 1b 18 b7 5f 03 4b a1 6a c5 7c c4 46 1e |.t...._K.j|.F.|
00002690 6b 09 51 77 6b 3b 0d 9c 17 36 31 71 07 f4 9a bb |k.Qwk;...61q....|
```





Problem: lots of & heterogenous data



Digital evidence

- terabytes of data, millions of traces
- multiple sources and formats

XIRAF

- processing input, automated forensic analysis
- data warehouse
- user tools
- modular architecture

Investigators

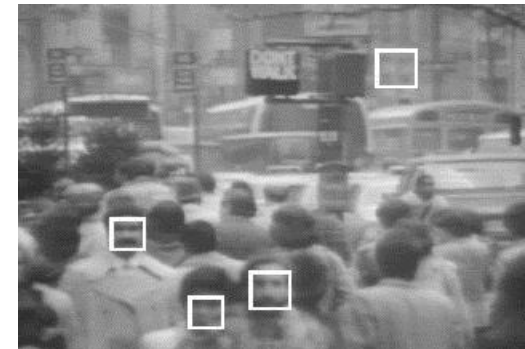
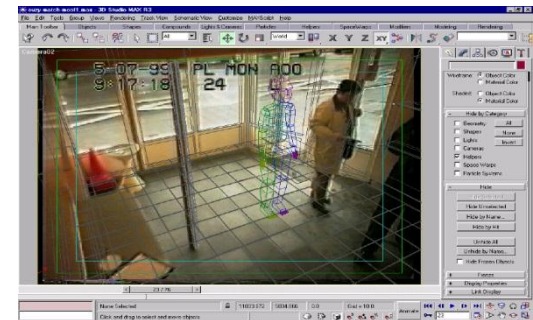
- (incremental) search, annotate, report
- via web interface



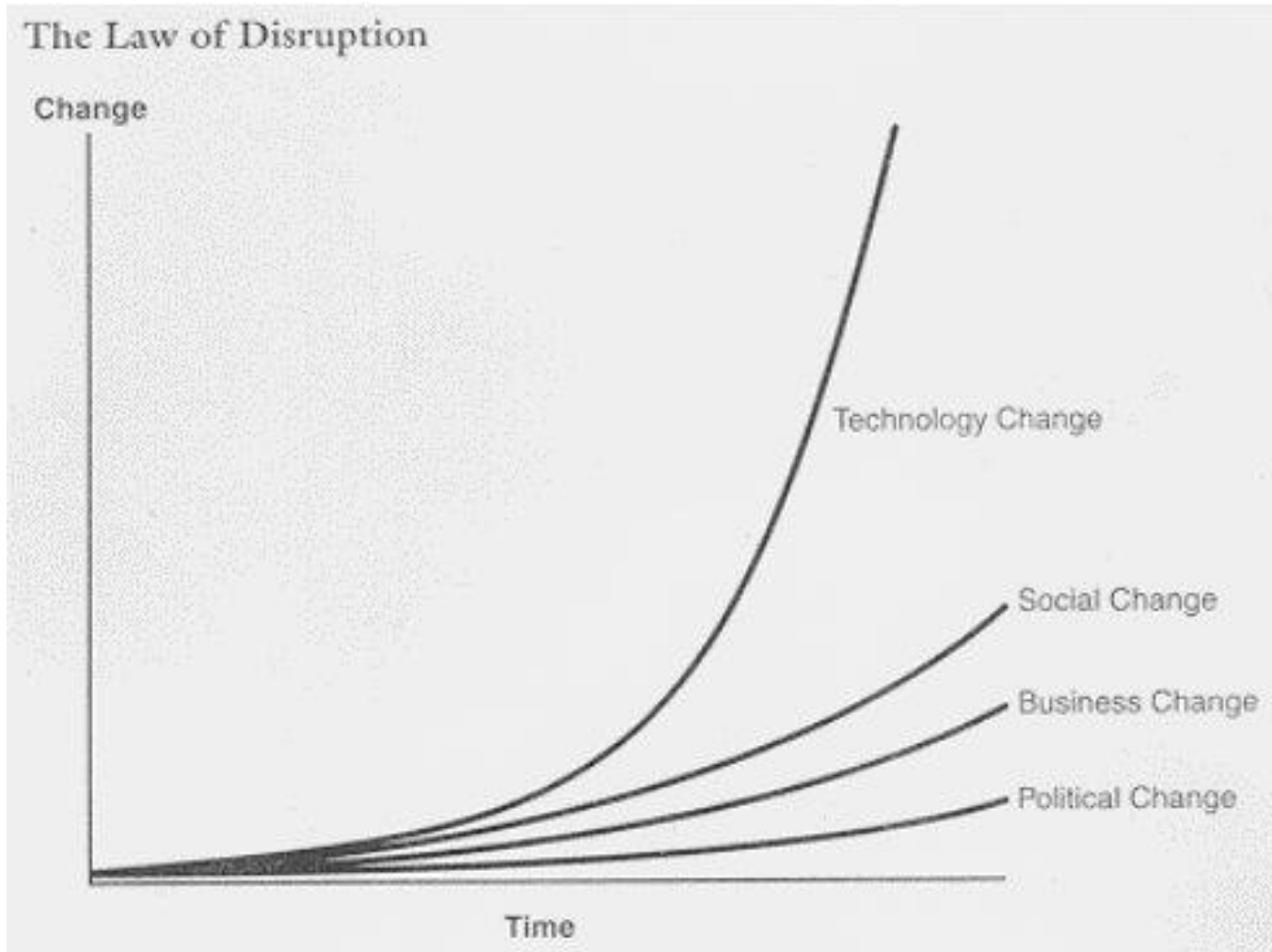
Problem: data are not self-explaining

Add models / analysis to support interpretation

- Scenario / timeline analysis
- Geographical models: e.g. location of cell phones
- Analysis of images / video / audio
 - Size
 - Speed
 - Face recognition
 - Speech recognition
- Decoding languages, author recognition
- Link to other forensic disciplines



Trends



Larry Downes. 2009



Challenges in digital forensics

Digital domain: Moore's Law (1965) applies

- Keeping up-to-date, war for talent
- Provide knowledge, methods, tools for police operations
- Standard work in efficient operations

Required: closer co-operation,
internationally and public-private





CSI The Hague

Digitize the crime scene: **fiction becomes reality**

The consortium

Netherlands Forensic Institute, TNO, Philips, E-Semble,
Noldus Information Technology, Chess Embedded Technology,
Thales Nederland, Eagle Vision, Forensic Technical Solutions,
Amsterdam Medical Center, Capgemini, The Hague University,
Delft University of Technology.



Netherlands Forensic Institute
Ministry of Security and Justice

Digital Forensics at NFI

Erica Rietveld
Manager Digital Technology
& Biometrics

Netherlands Forensic Institute

28 March 2011