Incident Erfahrungen / Forensic Readiness

Beer-Talk der Compass Security AG - 30. August 2012

- Stephan Rickauer -

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Agenda

Who am I?

Quick Introduction to IT Forensics

Incidents, Experiences, Cases

Forensic Readiness – Yet Another Buzzword?

Technology Demo: Log File Analysis

Technology Update: Solid State Drives

Beer? Meat?

Who is /me?

Quick Introduction to IT Forensics

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

History

“Forensics”

"pertaining to or suitable for courts of law," 1650s, from L. forensis "*of a forum, place of assembly,*" from forum "*public place*" (see forum). Used in sense of "pertaining to legal trials," as in forensic medicine (1845).

http://www.etymonline.com/index.php?term=forensic

History

Locard´s principle of the exchange of evidence:

Every contact leaves a trace

- Either the criminal leaves something behind
- Or the criminal removes something

This is true for the investigator too

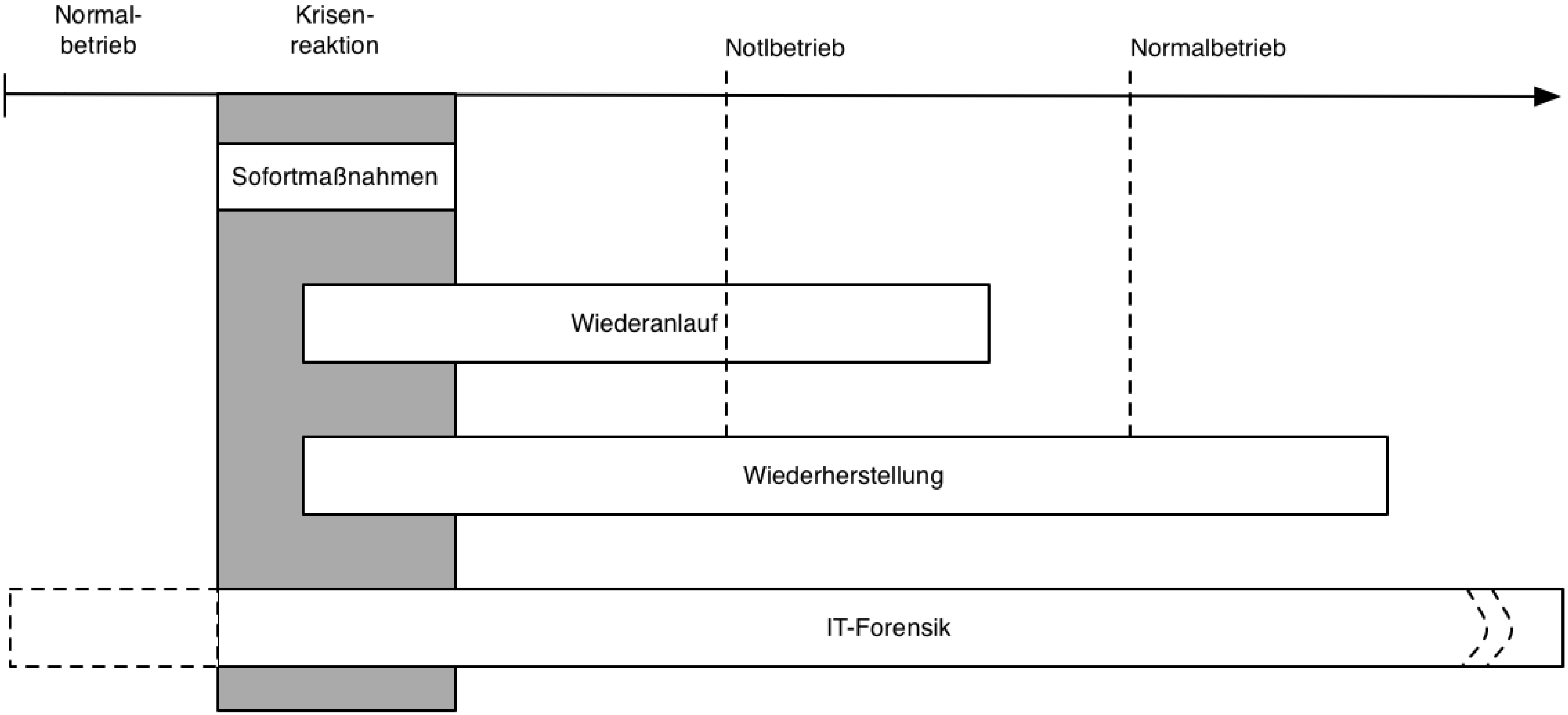
- Minimize own fingerprints
- Account every step taken with the evidence

Definition "Forensic"

Applies principles of forensics science to IT

> “Forensic Computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that **is legally acceptable.”**
>
> Rodney McKemmish (1999)

Forensics within BCM



BSI-Standard 100-4

Incidents, Experiences, Cases

Compass Security AG	Tel +41 55 214 41 60
Werkstrasse 20	Fax +41 55 214 41 61
Postfach 2038	team@csnc.ch
CH-8645 Jona	www.csnc.ch

Top Five Epic Fails

1. No or not enough data to analyse
2. Data to analyse not accessible
3. No clear project focus
4. Underestimated project costs
5. Too much data to analyse

Forensic Readiness -
Yet Another Buzzword?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Terms and Definitions

Computer Forensics is commonly employed as a reactive measure to serious information security incidents. All of a sudden, digital traces (evidence) need to be made available to investigators.

Problems:

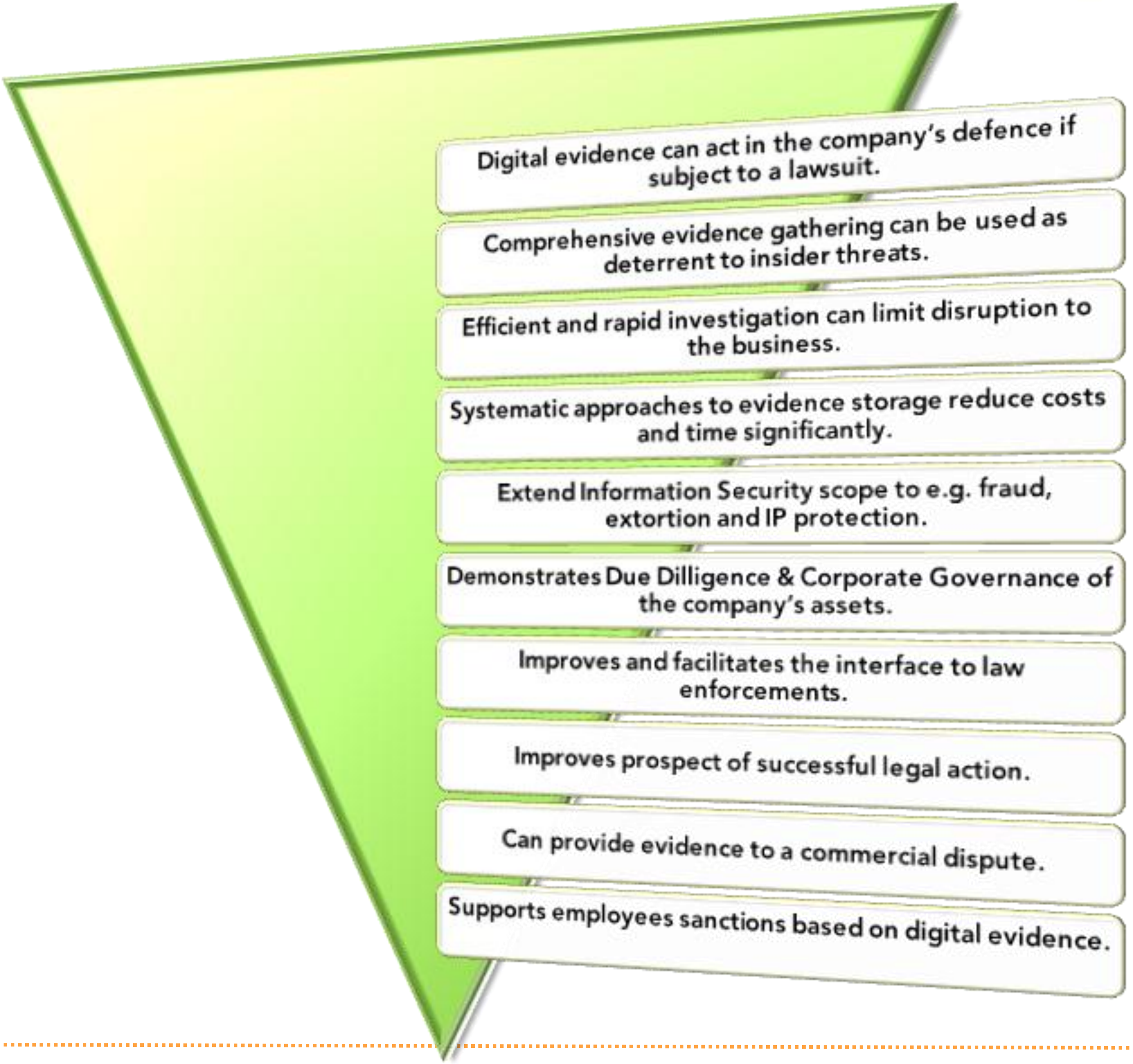
- Do you know where your data is?
- Do you know, where your **relevant** data is?
- How is it accessible? Live?
- Who can access it? Are those persons available now, on a Sunday?
- Is accessing that data actually legally permitted?
- How to you transfer the data to the investigators?
- ...

Terms and Definitions

«Forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.»

Robert Rowlingson, QinetiQ Ltd.

Benefits of Forensic Readiness



Digital evidence can act in the company's defence if subject to a lawsuit.

Comprehensive evidence gathering can be used as deterrent to insider threats.

Efficient and rapid investigation can limit disruption to the business.

Systematic approaches to evidence storage reduce costs and time significantly.

Extend Information Security scope to e.g. fraud, extortion and IP protection.

Demonstrates Due Dilligence & Corporate Governance of the company's assets.

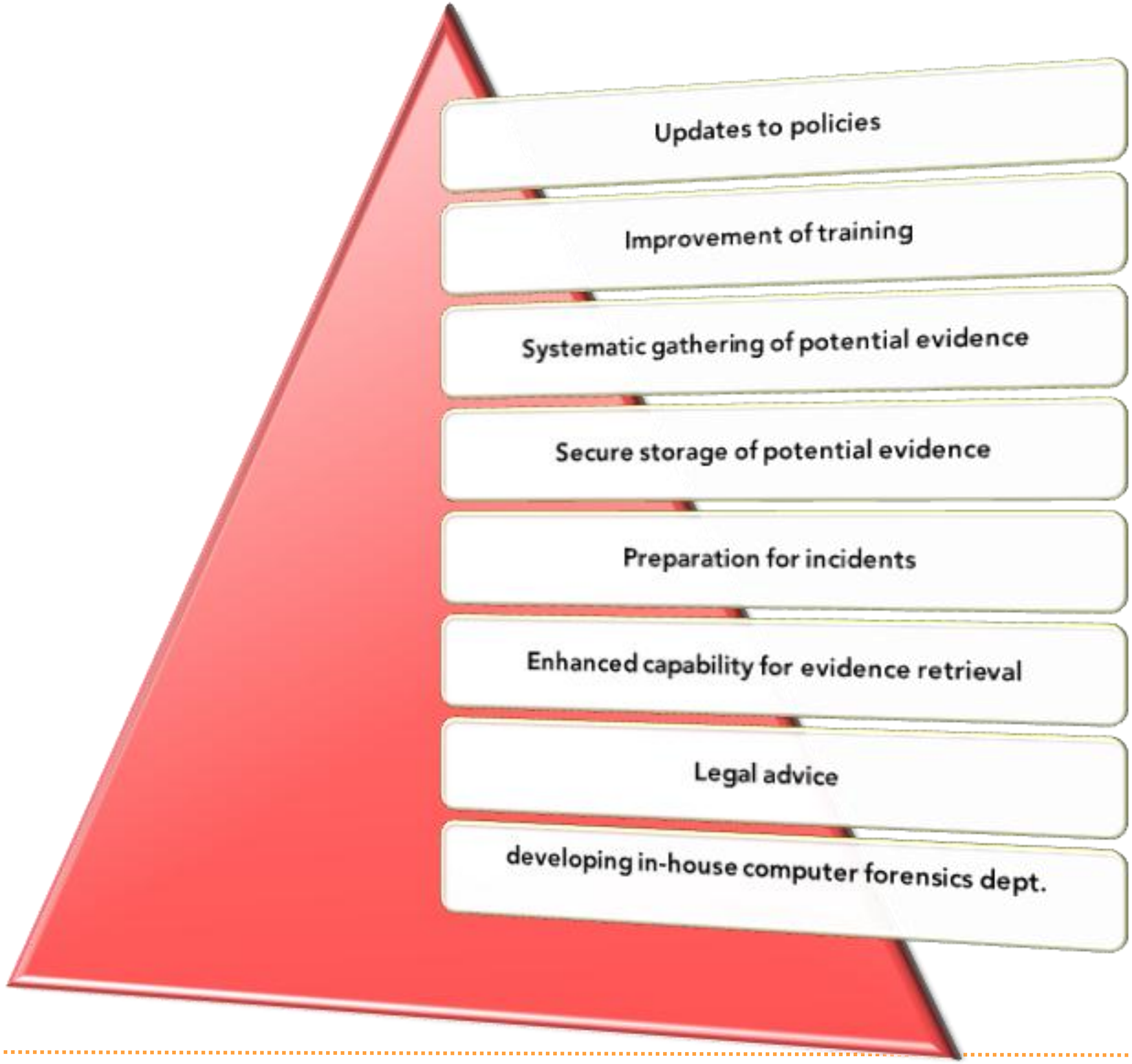
Improves and facilitates the interface to law enforcements.

Improves prospect of successful legal action.

Can provide evidence to a commercial dispute.

Supports employees sanctions based on digital evidence.

Cost Factors of Forensic Readiness



Updates to policies

Improvement of training

Systematic gathering of potential evidence

Secure storage of potential evidence

Preparation for incidents

Enhanced capability for evidence retrieval

Legal advice

developing in-house computer forensics dept.

10 Steps to Forensic Readiness

1. Define business scenarious that require digital evidence.
2. Identify available sources and types of potential evidence.
3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of evidence.
6. Ensure monitoring is targeted to detect major incidents.
7. Define escalation procedures for full, formal investigations.
8. Train staff incident awareness
9. Establish a documentation policy for evidence-based cases.
10. Ensure legal review to facilitate action in response to an incident.

Technology Demo:
Log File Analysis

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Goal

Find the IP address of someone with suspicious behavior and tell what s/he did. Further we want to know as many details as possible about the suspect's browser and operating system.

Technology Update:
Solid-State Drives (SSD)

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

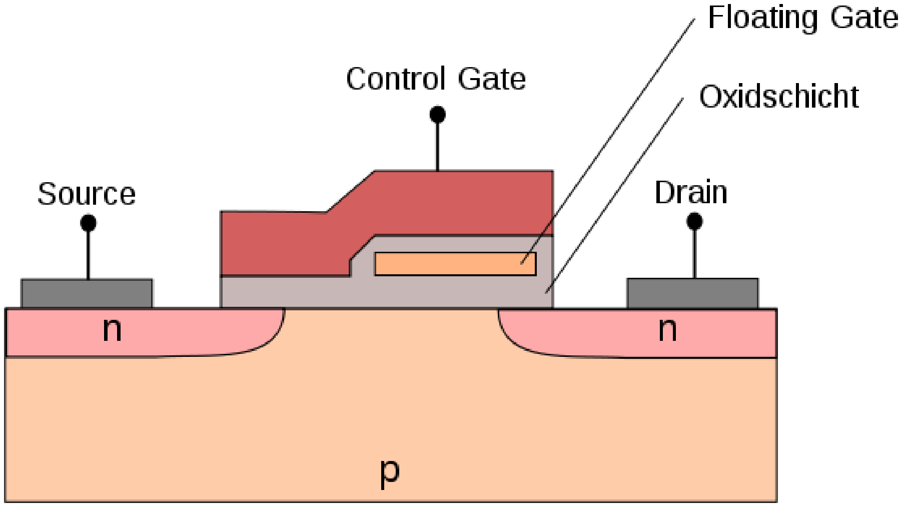
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

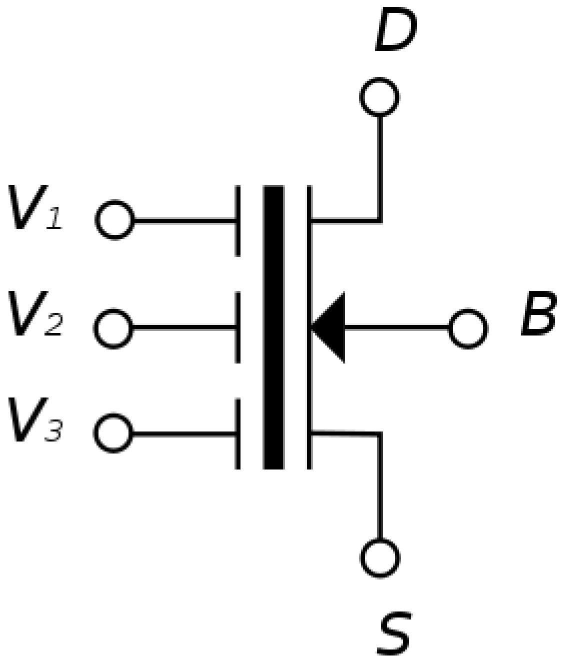
Solid-State Drives

Become more and more popular as replacement for magnetic hard disks:

- NAND-based flash memory
- No moving mechanical components
- Shock resilient, silent
- Lower access time and latency
- More expensive
- Two flavours: SLC and MLC

Principle of Floating-Gate Transistors



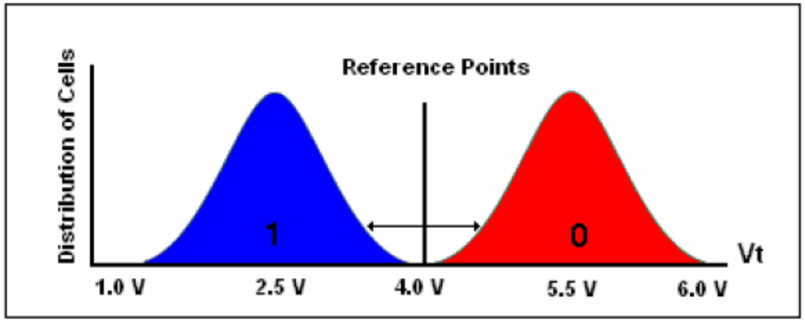


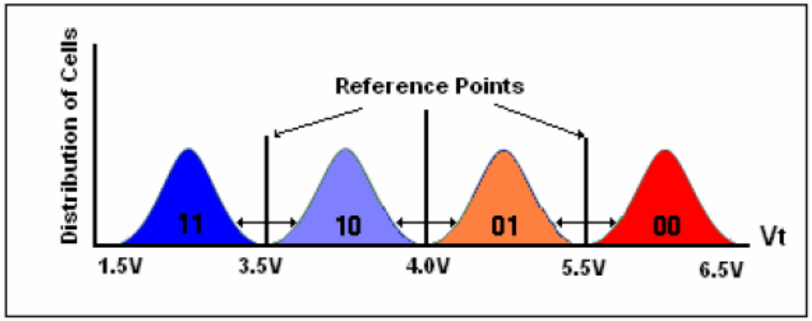
Source: http://de.wikipedia.org/wiki/Floating-Gate-Transistor

SLC vs. MLC

SSDs come in two flavours:

- Single-Level cell (SLC)
- Multi-Level cell (MLC)





	SLC	MLC	
Density	16Mbit	32Mbit	64Mbit
Read Speed	100ns	120ns	150ns
Block Size	64Kbyte	128Kbyte	
Architecture	x8	x8 / x16	
Endurance	100,000 cycles	10,000 cycles	
Operating Temperature	Industrial	Commercial	

Data structure

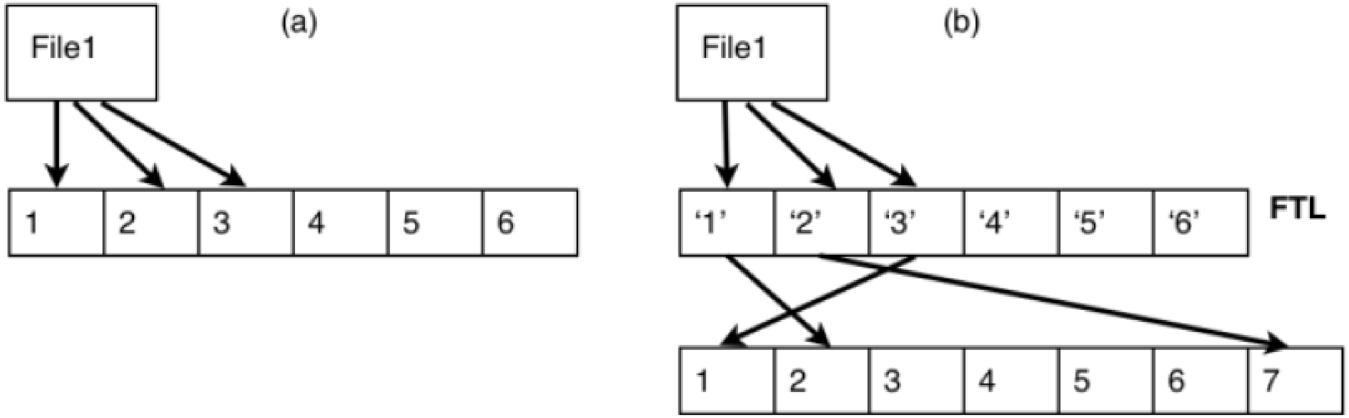
Flash organised by cells:

- Multiple NAND-cells built a “page” (usually 512B to 4kB)
- 64 to 128 pages are combined to a “block”
- A block in a modern SSD is usually 512KB
- NAND-flash can only read and write on a block basis

Forensic issues with SSDs: FTL

Flash Translation Layer (FTL):

- Due to wear, writes are levelled by FTL
- Two subsequent writes won’t end up on the same block
- The computer is unaware of where the data is stored



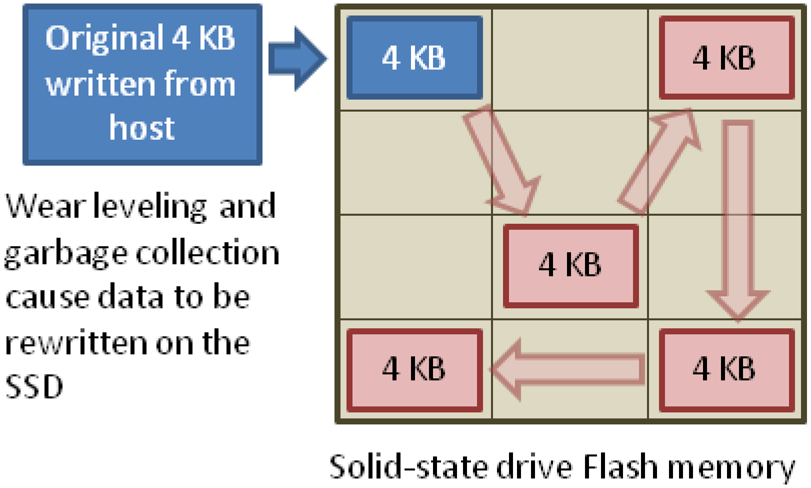
a) Hard disks

b) Solid-State Drive

Forensic issues: Garbage Collection

Garbage Collection fixes a number of problems by "cleaning up" in the background by the controller chip autonomously:

- The erase process is very slow (~10ms)
- Only entire blocks can be stored/erased
- The Read-Modify-Erase-Write problem



Original 4 KB written from host
Wear leveling and garbage collection cause data to be rewritten on the SSD
4 KB
4 KB
4 KB
4 KB
4 KB
Solid-state drive Flash memory

Forensic issues: TRIM

TRIM is an attribute of the ATA Data Set Management Command:

- Like Garbage Collection, but issued by OS
- Supported since Windows 7, Linux 2.6.33, OS X 10.6.8, FreeBSD 8.2
- “Online” or “Batched”
- Not supported by most RAIDs as of today
- UNMAP is the SCSI equivalent

Example Ubuntu usage:

```
# hdparm -I /dev/sda | grep -i trim
* Data Set Management TRIM supported
* Deterministic read ZEROs after TRIM
```

Recommendation and Guidance

1. **Consider SSDs as 'grey area' wrt to legal validation**
2. Corrosive data may get deleted extremely quickly
3. **Evidence of 'no data' does not prove data wasn't there**
4. Deleted data no longer evidence of human intention
5. Hashes may not match. Documentation/Peer-Review required.
6. **File carving won't work as usual**
7. Quick formatting must no longer distringuish from full format.
8. Write-blockers are not that useful any longer

Conclusion

“**It** seems possible that the golden age for forensic recovery and analysis of deleted data [...] may now be ending.”

Manche Sachen muss man nicht testen.

Andere schon.

References

- «A Ten Step Process for Forensic Readiness»,

  Robert Rowlingson, QinetiQ Ltd.

  https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

- «Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?»

  Graeme B. Bell, Richard Boddington, 2010