Digital Evidence Gathering

"*keeping the trail*"

Xander Beenhakkers
Jos Griffioen

March 17, 2006

Contents

Introduction

"**Evidence**: Information, presented in testimony or in documents, that is used to persuade the fact finder (judge or jury) to decide the case for one side or the other. (Source: Internal Information Programs US)

"**Information** has meaning (i.e.: can inform), while data does not."

"**Data** is the plural of *datum*. A **datum** is a *statement accepted at face value* (a "given")."

(Source: Wikipedia, the free encyclopedia)

Introduction

Data can be divided in three main categories:

- Physical; written text on paper, any object, etc.
- Mental; facts stored in people's minds
- Digital; bits in any electronic device.

Classification of Digital Data

- **Communication data**; fax, documents, e-mail, gsm,
- **Transaction/process data**; invoices, clients
- **Corporate Governance data**; authorisation and sec
- **Business Intelligence data**; data-mining
- **Software**; Erp-systems, word, etc.

Gathering info

Collection methods

- Imaging: Take everything
- Forensic copy: Take what you need
- Selection and extraction: large db, e-mail
- Making it physical and with testimony
- Edp auditing/forensic accountancy

Acquisition

Archiving tools and hashing data , testimony, logging

Analysis methods

- Identification; what is it?

  file recognition, re-construction.

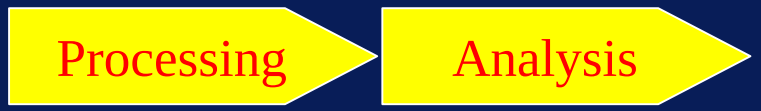
- Interpretation;

  Index search and reading, programs

- Pattern analysis;

  time-line, contact-circles

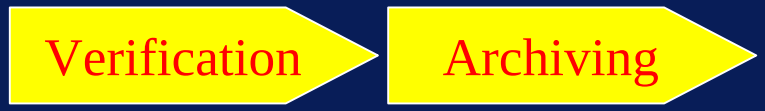
- Process analysis;



Hashing, Testimony, logging

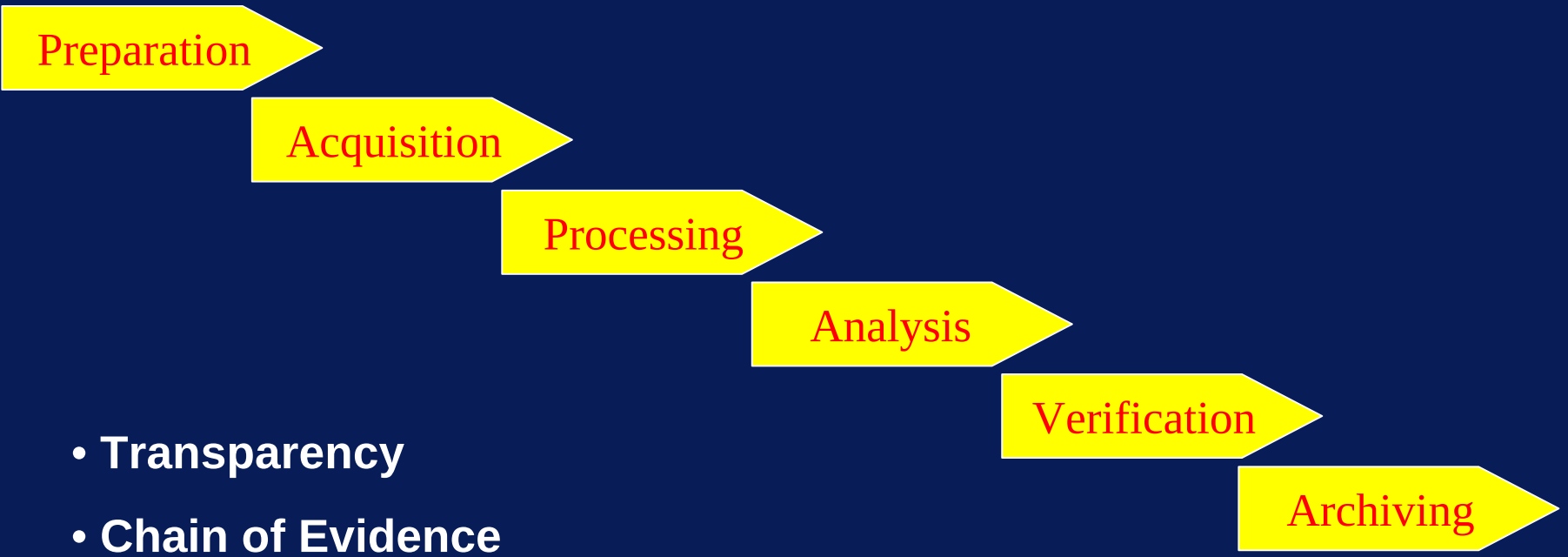
Keeping the Trail

- Verification;
- Validation;



Testimony, archiving

Keeping the trail



- **Transparency**
- **Chain of Evidence**
- **Chain of Custody**

Summary

- **The digital world is fully integrated in the analogue world**
- **The technology needed for investigation of digital data is commonly used**
- **It becomes natural that Competition Authorities act more and more in this diverse digital environment**
- **‘Keeping the trail’ is essential for the forensic value of digital evidence and a (future?) role for the IT-specialist as an expert witness**

Questions?