elaman
GERMAN SECURITY SOLUTIONS

Computer Forensics

Information

GOVERNMENTAL SECURITY SOLUTIONS

Why forensics?

To know how the attacker works

To acertain the loss

To identify the attacker

preservation of evidence

Who are the attacker?

Hacker/Cracker

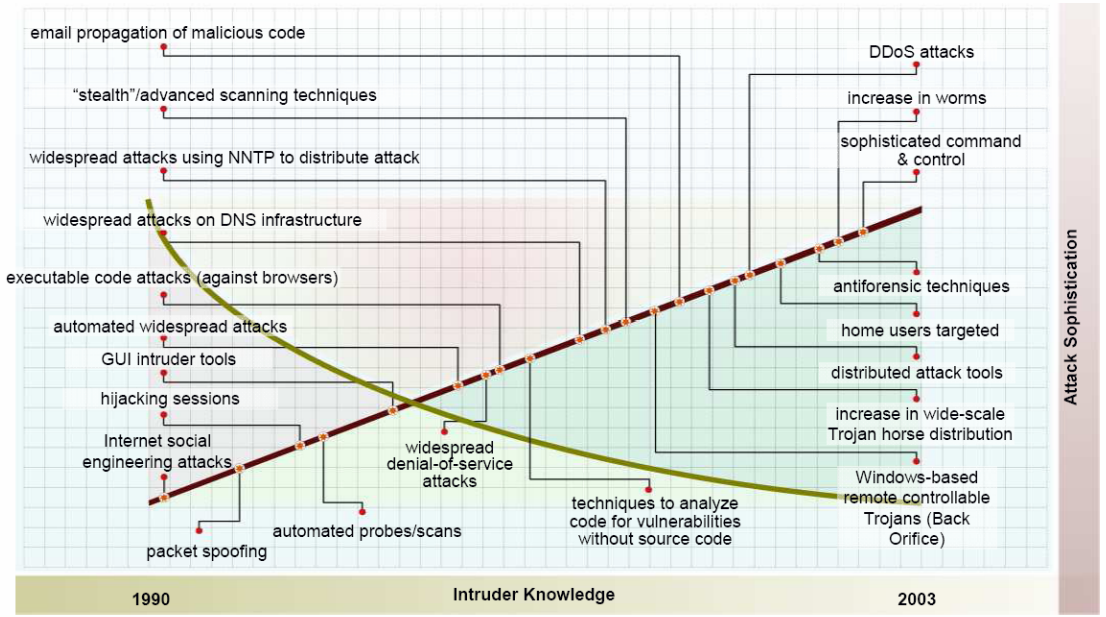
- Just for fun
- Politically motivated
- financially motivated

Staff members

competitors

Intelligence

Quality of the attacks vs. needed know how



Quelle: CERT

Basic questions

- **What was happened?**
- **Where?**
- **When?**
- **How?**
- **Who?**
- **Why?**

Forensic process

- **alert or incrimination**
- **Cost / benefit equation**
- **Secure „site of crime“ very difficult for the Internet**
- **Collect evidence (photograph, document)**
- **Protect evidence verifiable against modification**
- **Analyse data**
- **Appraisal of results**
- **Documentation and presentation of the results**
- **Testimony at court**

Collecting data

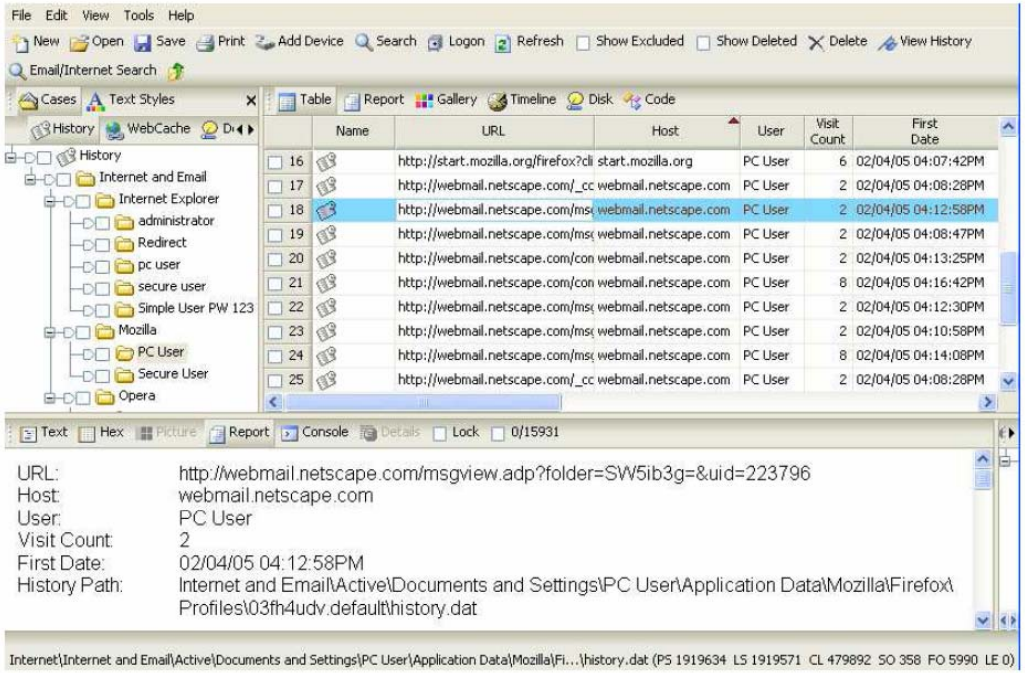
- **order**
  - Cache, RAM
  - Temporary files, actual state of the network, running processes
  - Hard disks
  - Floppy disks, CD/DVD-RW, USB-devices, ...
  - CD/DVD-R, paper
- **Save the data to a forensic workstation**

Tools (1)

- **From trustable source**
- **bootable CD/DVD (HELIX, FIRST)**
- **Unix/Linux**
  - dd, cp, cat, ls, ps, strings, find, file, bash, grep, less, vi, ifconfig, kill, nc/netcat, tcpdump, arp, df, diff, du, last, lsmod, md5, sha1, netstat, rpcinfo, showmount, top, uname, uptime, who, fdisk,
- **Windows**
  - Foundstone (z.B. FPort), Sysinternals (z.B.Handles,PsList) …

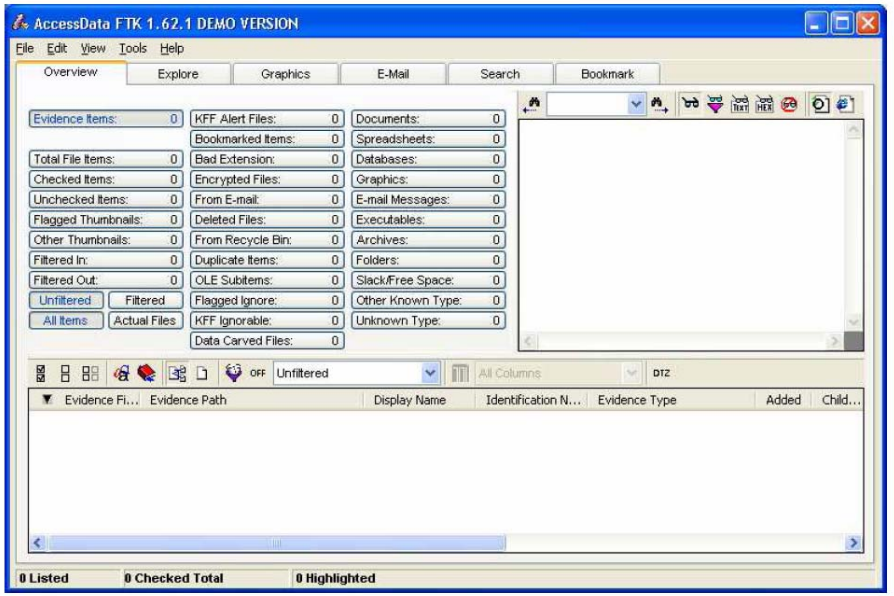
Tools (2)

- **Encase**



Tools (3)

- **Forensic Tool Kit**



Site of crime

Keep cool!

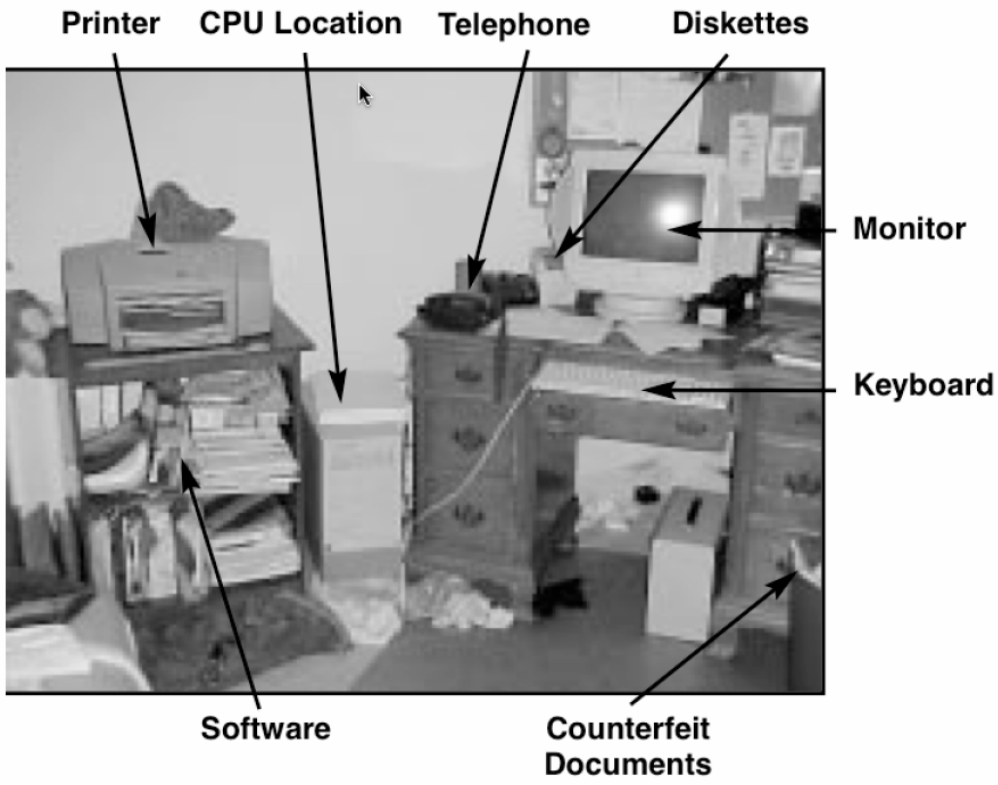
decisions

- Turn off the System or not? (memory, Processes)
- Plug off the network? (network connections)

Photograph and document everything

Save the evidence

Site of crime



Volatile data

- **RAM**
  - dd bs=1024 < /dev/kmem | netcat –w 2 [target-IP] 1234
- **Network connections**
  - Netstat -an | netcat –w 2 [target-IP] 1234
- **miscellaneous**
  - last, who, w, ps, lsof, arp, ...
- **External sources: Logserver, Firewall-, Intrusion Detection and Router-Logfiles**

Non-volatile data

- **Create checksum of the data (sha1 oder md5)**
- **Create a Bit-by-Bit copy of the source**
- **Create checksum of the copy and compare it with the original**
- **Why 1:1 Image and not a simple copy?**
  - File Slack (not completely written cluster)
  - no modification of the access times (MACtimes)
  - • M – mtime: change of the content
  - • A – atime: last read access
  - • C – ctime: change of the Inode (rigths, owner)

Forensic copy

- **Writeblocker**
  - Hardware
  - Software
- **requirements**
  - Creation of a bit-stream-duplicate or an image from an original hard drive/partition
  - No modifications on the original hard drive or partition
  - Read/write errors have to be logged
  - Documentation must be complete and correct

Questions for the examination

- **What was saved on the hard disk?**
- **What traces did the applications leave?**
- **What files were deleted?**
- **Are there hidden files?**
- **Are encrypted files or scopes on the disk?**
- **Subsist hidden partitions?**
- **Subsist backdoors or remote admin tools?**

Analysis

- **Search and examine all log files**
- **Search for particular keywords**
- **Examine all relevant data**
- **Identify not authorised user and group accounts**
- **Identify suspect processes**
- **Check unauthorised access**

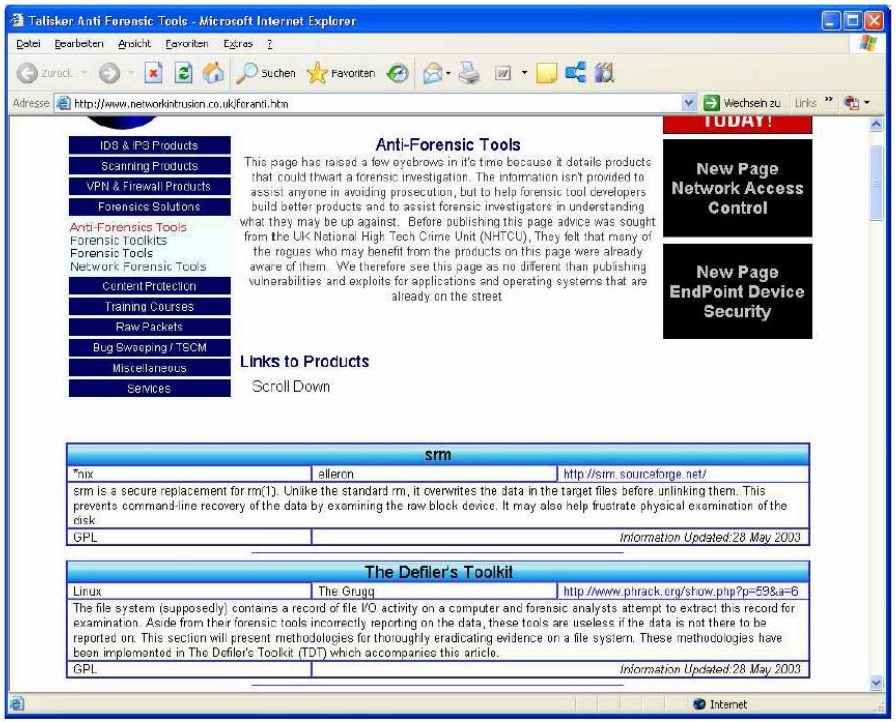
Presentation

- **Present not only findings ...**
  - But rather how you did it
- **Show the rules and standards you have used**
- **Substantiate the conclusions**
- **And alternative explanatory models.**

Criminal prosecution

- **Who makes the decision?**
- **Criminal or private law**
- **Complaint of an offence**
  - Will you do it?
  - Who can do it?
- **Site of crime principle**
  - Where is the offender?
  - Where arose the damage?
- **Collection of evidence (own team or police authorities)?**

Limitations by antiforensics



GOVERNMENTAL SECURITY SOLUTIONS




If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de