

# Digital Forensic

Lukas Grunwald

*DN-Systems GmbH*

*Hildesheim, Germany, 31137*

`l.grunwald@dn-systems.de`

`http://www.dn-systems.de/forensic`

**Draft of 2004/01/31 20:34**

## Abstract

The methodology of Digital Forensic can be compared to the method of a criminologist although the tracking and conservation of evidence of the inside of a computer that has been the target of or was used for an attack is far more complicated.

## 1 Introduction

Over the past few years the internal and external law enforcement agencies have registered an increase of crimes where computers and computer systems have been involved. These criminal deeds include fraud concerning 0190-dialers, illegal disspreading of pornographic material such as child or animal pornography, the falsification of financial statements and operating data, the spreading of computer viruses in order to attack computer systems. Facing the increase of such crimes the term computer gets a whole new meaning in investigations and in court. As soon as investigations start when someone has committed a crime by using his computer to manipulate or compromise a computer system, a technical and criminological procedure begins - the so called Forensic Computing, quite often also referred to as Computer Forensic or Digital Forensic. The realm of this fairly new discipline has not yet been completely defined. The author Michael Caloyannides, an expert in this field, defines it as the collection of all methods and tools for the purpose of searching for evidence. But this definition is only partly appropriate. In addition to searching and securing digital traces, one should not underestimate the importance of preparing the facts in order to obtain an expert opinion that can be used in court. Evidence is the key word: The forensic specialists are confronted with the challenging task of presenting technical facts and evidence in such a way that they become comprehensible to a jury without technical expertise in court. Documentation is just as significant in forensic analysis as is the technical finesse in finding and securing evidence. Every step in securing of evidence and investigation has

to be recorded precisely for the purpose of subsequent traceability. While analyzing a computer several pieces of data are collected that can reveal information about the user. They can also be used as evidence if necessary. Among them are the processor ID, the swap or page field, the file system, token, flash memory as well as the MAC address of the network adapter. In addition to this you can also investigate tangible sources of information found in close proximity to a computer of interest: Notes, printed documents, contents of PDAs or listings of cell phone numbers left behind on a desk. All these data sources may contain vast quantities of information that can be correlated with data found on a computer.

## 2 Preserving of data

At the beginning of any forensic analysis the experts need to investigate all the data on hand and to secure the various data media. In order to preserve the original evidence and to prevent a potential damage during the analysis, the forensic analysis is usually carried out on a copy of the secured data. In order to make a copy the expert clones the hard disk on the physical and logical block level using a special tool that is typically included in a forensic-toolkit. On this copy the forensic analysis can be performed in a read-only-modus. We recommend selecting the tool with great care: Some cloning methods destroy the metadata that are required for a successful forensic analysis. If computers are confiscated in cases of tax fraud, imposture of contracts or other felonies securing data can be carried out quite easily. The cloning and forensic analysis of data can then be performed without any pressure of time. It is far more complicated to trace an incident or rather various processes if a hacker has attacked a system. When the attack was finished before it has been detected the experts generate a copy of the involved processes by using an appropriate forensic tool. With Linux it is possible to create such a copy by using the `dd` command and the `/proc` file system.

### 3 On-the-fly Securing of Evidence

When an attack has not been finished yet the administrator has to make an important decision. In such a case forensic experts usually recommend to immediately separate the affected computer from the network. In this way not only the attack is stopped but it is also prevented that the hacker can delete his or her revealing traces. If, however, the computer stays online there is a chance of identifying the intruder's connection or to save a copy of the main memory to hard disk. The administrator has to decide on the pros and cons for either strategy within a matter of seconds. He also has to be prepared to revise his decision if necessary, for example to cut the connection when a hacker tries to delete or to reformat data. And even then the integrity of the data can not be guaranteed. In the worst case the attacker has infiltrated a cronjob that covers or destroys his traces. In such case the system's current state should be immediately frozen in order to provide some sort of snap shot for the forensic analysis. Any modification of data - often unintended - can make data useless as evidence. For example, restarting a Windows 2000 system causes modifications to 192 files. Therefore you should avoid rebooting a computer that was shut down. Instead, the analysis can be performed after the hard disk had been removed using a secondary analysis system. By contrast, you should avoid shutting down a computer that is still running: The system would delete all temporary data such as cache contents or certain log files. Incidentally it also happens that the main memory swap area is overwritten.

#### 3.1 Fire resistant Hard Disks

While a still running computer might require special measures, securing data usually takes place by order of transience: At first the data of transient caches, main memory and running processes are secured, then the data of hard disks, CDs or floppy disks. Efforts and expenses spent on such analysis may depend on many factors:

- Keep calm and avoid taking unadvised steps.
- Amount of money involved.
- Type and severity of felony.
- Personal and private motivation.
- Other different factors.

If the hard disk is damaged the physical access to the data has to be restored in a data recovery lab before any further analysis can take place. Thanks to state-of-the-art technologies there is quite a good chance of being successful. And if a culprit thinks he could destroy evidence by setting a system on fire he is definitely wrong. Modern hard disks are able to withstand fire for several minutes before reaching the critical temperature where its magnetic storage medium starts losing information. Usually it is possible to restore most if not all

data. After collecting and securing all evidence you can start analyzing the data. Computers store files on a hard disk in different steps using various layers of abstraction. When extracting information, experts usually follow a top-down approach. A starting point could be searching normal files for evidence, accessing them by using the system's standard software tools. As a next step deleted files can be restored by using special tools in order to make them visible and accessible again.

Step 6 can also be revealing in other respects. You can analyze access authorization and - under Unix - different kinds of time stamps. Utilizing this method you can gather various information about a file: When the latest changes have been made (M-), when the last access took place (A-) and when the file has been created (C-). If you can rule out that someone has manipulated the metadata containing these time stamps the person analyzing the data is in a position to reconstruct file access in great detail. If this is not the case it has to be arched for evidence proving that someone has manipulated the metadata or file systems and in which way.

It is always possible that file names and directory entries are not available for reconstructed files. In this case the expert tries to find evidence by using a pattern recognition searching method. The headers of several file formats contain information on characteristic data structures such as color depth and resolution of image files. If it is suspected that there is forbidden pictorial material on a certain computer it is possible to search for this material by using this method. The disadvantage is that you have to look manually at every single picture. Very rarely a file header reveals additional meta information such as its creator or source server. Textual data can be searched for special terms or key phrases depending on the kind of offence. As different forms of encoding are in use it is advisable to generate patterns on the basis of different versions of encoding of a term. The sample search is performed on the logical level by using a forensic tool.

### 4 Client and Server Analysis

Depending on the kind of machine that is to be investigated you can distinguish between client and server forensic. The former kind of forensic analysis is more appropriate when you are searching for evidence of possession or distribution of illegal data contents. In order to arrest a person possessing pornographic photos of children German law enforcement agencies use a program called Perkeo (= Programm zur Erkennung relevanter kinderpornografischer eindeutiger Objekte = a program for unambiguous recognition of pornographic photos of children) that was especially developed for this purpose. One of the hurdles using this program is not a technical but a legal one: As the possession of this

kind of pictures is liable to persecution it is not allowed that the software includes respective pictures to use as a sample. Therefore Perkeo cannot recognize forbidden graphical material per se but only material that is already known and classified on the basis of digital checksum method.

Besides these weaknesses of this kind of software you have to take into consideration that the computer of a user can be abused for exchanging forbidden material without his knowledge via a security weakness for example of a chat program such as mIRC. A security analysis of the PC that reveals all incriminating and relieving facts can help to unearth the truth. Such a security analysis has to consider all communication channels of a computer: This includes modem and dial-up network as well as the connection to the internet, even to a printer. It also takes into consideration the search for security vulnerabilities that could have been used by an intruder. Log files such as the event log in Windows NT or sys log in Unix can also be helpful. They contain several pieces of information that are relevant for the analysis, among them: When and how often a user logs on and off and at what time the PC was online and so forth. A 65-year-old administration employee of an American university was dismissed as she had been accused of having stored pornographic pictures on her computer. The client-analysis brought it to light: As she had missed to log off her computer the cleaning personnel could abuse her account for browsing the Internet. Analyzing the server can also help to take hold of an intruder as the following example shows: One morning an administrator found on the console of his company's web server the following announcement: Someone owns this host! A root login led to the message: You don't exist, go away! When they tried to reboot the server the boot-loader stood still with kernel-panic. At the following examination they found out that there was still a file system, only the UNIX file system (UFS) was empty. A hacker had entered the clear instruction `rm -rf`. The analysis of metafiles and file server allowed backtracking the attack. Log and history files from the shell that were used by the hacker did not only reveal the course of the attack but also the hacker's source IP address.

When additional information of firewall systems or routing and accounting data is also available it is possible to perform forensic accounting. Forensic accounting data possibly allows to track the source of an attack or the hacker as far as he had not used another hacked computer as starting point for his attacks.

## 5 First Aid for Administrators

When you discover an attack on your system:

- Keep calm and avoid taking unadvised steps.
- Depending on the kind of situation it is advisable to

cut the connection to the internet in order to prevent further incidents or the covering of tracks.

- Secure log files of the firewall and other systems that have not been compromised yet.
- Make protocols of all incidents together with the exact point of time.
- Secure all data as soon as possible independently of the daily backup.
- Make physical copies with all metafiles when necessary.
- It is not advisable to carry out an analysis yourself when you do not have the technical knowledge but to contact an expert.

At the actual crime scene it is important to determine who has access to different rooms and computers or how access and execution rights are distributed within a company. This way it is possible to restrict the number of suspects. The final step after analyzing all data is the preparation of all gathered evidence and facts for an official expertise that can be used in court.

The criminological investigations are carried out in general by the police. Therefore, the official expertise of the forensic specialist is limited to technical evidence. How difficult it is to communicate this to non-technical people that are involved in this process is proven by the not uncommon request for printing out the whole content of a hard disk as reported by the data securing company ibas. In case of a modern 80 GigaByte hard disk the printout would result in a pile of paper amounting to the height of Mount Everest.

## 6 Translation of Technical Facts

The translation of technical facts into comprehensible examples is very time consuming says Thomas Schwarze, head of the department for forensic communication and information technology of the police Department of Hamburg.

The making of an expert opinion takes approximately as long as the actual investigation. Nevertheless the effort seems worthwhile: If there is clear evidence and it comes to legal proceedings, in general it is managed to translate the technical facts appropriately and the prosecution wins the case.

As attacks on computer systems ,despite precautions, cannot be eliminated completely, administrators should take those steps in time that facilitate forensic analysis. As a first step it is important to develop a security policy with security guidelines. The emergency plan that covers the issue of incident response (response to a security incident) is an important part of it. This concept defines in detail so called alerting chains, areas of responsibility and related proceeding. Users should be sensitized for security subjects and be familiarized with the company's security policy. As a next step the person respon-

sible for the system should document the entire network with all its active components. Security change management guarantees that the documentation is up-to-date. It is important to perform a risk assessment for each sub systems and its components and to provide them with security appliances such as an intrusion detection system or a firewall depending on the desired level of security.

## 7 Central Collection of Evidence

For subsequent backtracking of incidents it is important to know what happened and when. Each of the newer Microsoft operating systems (such as Win2k or XP), all derivatives of Unix, Novell Netware and Cisco IOS supports the Network Time Protocol NTP ([www.ntp.org](http://www.ntp.org)). It serves as basis for the implementation of a centralized time stamp mechanism that records every access and change of data and any other events with exact date. The reference time can be received either via a radio controlled clock (DEC77/GPS) or in case of systems with a leased line by the server of the German Physikalisch-Technische Bundesanstalt in Braunschweig ([ntp1.ptb.de](http://ntp1.ptb.de)). It is also advisable to operate a central log server. Using a secure procedure it collects all log messages from the network (server farm) and writes them to tamper-resistant media such as a virtual WORM-drive (write once read many). All recorded events of the fire wall, the intrusion detection system as well as log messages from single servers are correlated here. As a result it will be more difficult for an intruder to cover his traces. In order to discover spoofing of an operating system, as done by rootkits, the administrator of a system should create a list of MD5 checksums of all system binaries and the system core at a cleanstate. In case of an attack you can compare the checksums to see which data has been changed. Even if the measurements mentioned above help to improve securing evidence in the worst case there can be obstacles. One of the subtle difficulties that can get in your way are the different encodings when storing data depending on the kind of operating system (ASCII under DOS, EBCDIC with IBM Mainframes, AS/400, Unicode under Linux, Windows 2k and XP). Despite that, there is still a large number of binary formats. With picture and sound files on the system the number of binary formats gets even larger. The analysis is hampered as well by encrypted data systems such as produced by PGP. There are no guaranteed prospects for success but in case of additional efforts even encrypted data can be used. To avoid that the forensic specialists have to examine manually all sectors of the hard disk there are tools and collections of tools that can carry out different steps of analysis. Nevertheless further knowledge of operating and file systems, networks as well as file formats and metadata is essential to perform a successful forensic analysis.

## 8 Looking into a Tool-Box

You can find one example of such a collection of tools on The@tstake Sleuth Kit (TASK) where the IBM Public Licence Version 1.0 is available for everyone. TASK is based on the two years old The Coroner's Toolkit (TCT) the first available forensic tool collection. This collection consists partly of Unix commands such as file that try to determine the type of a file based on its initial part. By leveraging this command a specialist is in a position to analyze the image of a hard disk that was cloned using dd under Unix. An image cloned by TASK displays the following contents of the main directory:

```
[root@]# fls -f ntfs /winxp.dump
r/r 4-128-4:      $AttrDef
r/r 8-128-2:      $BadClus
r/r 8-128-1:      $BadClus:$Bad
r/r 6-128-1:      $Bitmap
r/r 7-128-1:      $Boot
d/d 11-144-4:     $Extend
r/r 2-128-1:      $LogFile
r/r 0-128-1:      $MFT
r/r 1-128-1:      $MFTMirr
r/r 9-128-0:      $Secure:$SDS
r/r 9-144-1:      $Secure:$SDH
r/r 9-144-2:      $Secure:$SII
r/r 10-128-1:     $UpCase
r/r 3-128-3:      $Volume
d/d 21344-144-1:  .ssh
d/d 3241-144-6:   Documents and Settin
r/r 3223-128-1:   hiberfil.sys
r/r 27-128-1:    pagefile.sys
d/d 3640-144-6:   Program Files
d/d 9627-144-1:   RECYCLER
d/d 9382-144-1:   System Volume Inform
d/d 19996-144-6:  tmp
d/d 11772-144-5:  wincmd
d/d 28-144-6:    WINDOWS
d/d 9820-144-5:  WUTemp
```

From this image you can extract all required data and metadata provided that the original hard disk was readable. Otherwise the skills of a data-rescue-team are required once again. For those who like it more comfortable: There is also a graphical frontend for TASK called Autopsy. The commercial toolkit En-Case Forensic 3.0 is very popular as this all-in-one collection does not require any Unix-skills. Thanks to this tool collection you are able to clone hard disks and perform an analysis on the image as well as search for images, documents and other patterns.

One special feature of EnCase allows you to search for files whose file extension is not in line with its contents. This program easily recognizes a JPEG file that was renamed readme.doc in order to conceal it. EnCase can

also search for email attachments in Outlook-Express folders. By using a boot disk only it can be started on a system without any additional installation. You can search for evidence via a network, parallel port or serial connection from a mobile investigation PC. This tool kit is especially intended for the investigation of Windows-Client-PCs but it also works with Mac OS and Linux systems as well as CDs and DVDs.

## 9 Forensic Work of the Police

An employee of a software company gave notice to quit his job and established a company of his own. Only shortly after this company sells its own software that looks very similar to the software of the other company. Like a scene from a spy film? Far from it! This withdrawal of company secrets is one of the most common crimes that are investigated by the department for forensic communication and information technology (abbreviated IuK = Forensische Kommunikations- und Informationstechnik) of the regional Criminal Investigation Department of Hamburg. The odds of proving the theft of intellectual property or other company secrets are quite good, reports Thomas Schwarze, head of the department. The offenders often leave a vast number of traces on their computers. Since mid-eighties all regional criminal investigation departments have founded departments that focus on crimes associated with computers. Today each regional criminal investigation department has its forensic communication and information technology department. Yet their equipment and organizational structure is anything but uniform. Whilst in several federal states of Germany a great part of the analysis is carried out by external companies, in Hamburg nearly all examinations, including expert opinion and legal action, are performed by experts. An ever increasing number of computer related crimes and the rapid development of technology demand for regular training of the forensic experts. According to Mr. Schwarze, further training represents one-third of the working hours. The remaining two-thirds are applied in equal shares for writing expert opinions, preparing legal action and presenting cases in court. Sufficient funds for the increasing demand of staff and know-how are only available in very few regional criminal investigation departments.

In addition to the difficulties mentioned above the officials have to overcome every day difficulties: In case of accounting fraud of attorneys, tax consultants or physicians, the officials would have to confiscate and take away their computer systems. But in this case the parties involved would not be able to go on working. A compromise must be found: Only dispensable computer systems are confiscated. In order to examine the remaining ones as well, clones of the hard disks of these systems are made on the spot. A more serious problem is the pro-

tection of data privacy: Sensitive data such as financial, medical and other data is stored on these computer systems that should not be seen by others. Searching the data base for evidence it is inevitable that the officials get access to this type of data. An answer to this problem has not been found yet. Nothing can be done except relying on the official's obligation for discretion.

Despite all difficulties Thomas Schwarze is quite satisfied with his team. Those cases that are submitted to a court are fought successfully due to forensic securing of evidence. Most of the offenders who are caught in Hamburg are so called script kiddies. According to Thomas Schwarze this reveals nothing about the profile of the offenders in general. Those offenders who have specialized knowledge will not be caught.

## References

- [1] The Coroners Toolkit  
<http://www.fish.com/tct>
- [2] @STAKE Toolkit  
<http://www.atstake.com/research/tools/task/>
- [3] Forensic Toolkit  
<http://www.guidancesoftware.com>