

Searching for Evidence
Digital Forensic Analysis
draft

Lukas Grunwald

CTO

January 26, 2004

Contents

1	Introduction	1
2	Preserving of data	3
2.1	On-the-fly securing of evidences	3
2.2	Fire resistant hard disks	4
3	Client and Server Analysis	6
4	First Aid for Administrators	8
5	Translation of technical facts for technical laymen	10
6	Central collection of evidence	11
7	Looking into a forensic specialist's tool-box	13
8	Interview with Thomas Schwarze	15
8.1	Forensic work of the police	15

Chapter 1

Introduction

The method 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 had been the target of or was used for an attack is far more complicated.

Over the past few years the internal and external law enforcement agencies have registered an increase of crimes where computers and computer systems had been involved. These criminal deeds range from frauds concerning 0190-dialers, illegal disspreading of pornographic material such as child or animal pornography, the falsifying of financial statements and operating data, the disspreading of computer viruses in order to attack computer systems. Facing the increase of such crimes the term computer gets another meaning in investigations and in court. As soon as the investigations start when someone has committed a crime by using his computer to manipulate or to 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 topics of this fairly new discipline have not yet been completely defined. The author Michael Caloyannides, an expert in this scientific field, defines it as a collection of all methods and tools for the purpose of searching for evidence. But this definition is only partly appropriate. In addition to the searching and securing of the digital tracks, there is also the preparation of 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 the technical facts and evidences in such a way that they become comprehensible even to non-technicians among the participants in court. The documentation is

also part of the forensic analysis. Every step of the securing of evidences and the investigations has to be recorded exactly for the purpose of subsequent traceability. While using the computer several 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 consult data media, notes, print documents, contents of PDAs or telephone lists of mobile phones numbers at the desk for the purpose of the investigations. All these data contain a large number of information that should be correlated with data that have been found on the computer.

Chapter 2

Preserving of data

At the beginning of the 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 evidences and to prevent a potential damage during the analysis, the data the forensic analysis is 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 also included in the forensic-toolkit among others. On this copy the forensic analysis can be performed in the read-only-modus. We recommend selecting the tool with great care: Some of clone methods destroy those metadata that are required for the forensic analysis. If the computers are confiscated in cases of tax evasion, imposture of settlements or other offenses the securing of the data can be carried out quite easily. The cloning and forensic analyzing of the 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 had 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.

2.1 On-the-fly securing of evidences

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 the computer stays online there is on the other hand the possibility of to identify the connection data of the intruder or to save a copy of his main memory to their hard disk. The administrator has to decide on the benefits and damages within a matter of seconds. He or she has also to be prepared to cancel his or her decision in case of need and to cut the connection when the hacker tries to delete or to reformat data. And even then the integrity of the data can not be guaranteed. At the worst the attacker has infiltrated a cronjob that covers or destroys his traces. The systems final state has to be immediately frozen in order to provide some sort of snap shot for the forensic analysis. Any modification of data - even by accident - can result in the fact that the data become useless as evidence, such as a restart of the system under Windows 2000 causes a modification of 192 files. Therefore you should avoid the rebooting of a computer that was shut down the analysis can be performed after the hard disk had been removed. The other way round you should avoid shutting down a computer that is still running: The system will delete all temporary data such as the cache content or some log files incidentally it also happens that the main memory swap area is overwritten.

2.2 Fire resistant hard disks

Apart from special cases of still running computers the data securing takes place in the order of their transience: At first the data of transient cache contents, main memory and running processes are secured, the data of the hard disk, of CDs or floppy disks are secured in the final step. The efforts and the expenses of such analysis depend on the respective requirement. If the hard disk is damaged the physical access to the data has to be restored in data recovery labs first of all. Thanks to best available technologies there is quite a good chance of being successful. And if a culprit thinks he or she could destroy evidences by setting them on fire he or she is definitely wrong. The nowadays produced hard disks can stay on fire for several minutes without reaching the critical point of temperature on which a magnetic storage medium loses its information. You can restore at least most of the data (see figure 1). After collecting and securing all evidences you can start to analyze the data. The storage of a file to a hard disk is accomplished in different steps and in various levels of computer. Out of these the information were extracted by the expert in general by using the top-down method.

He starts with searching normal files for evidences that can be accessed by using the system software tools (step 7 in figure 3). If it is not possible to find evidences, the next step will be to treat deleted files by using special tools in order to make them visible and accessible again (step 6 of figure 3).

Step 6 is also in other respects informative. You can analyze in this step access authorization and - under Unix - different kind of time stamps. By this method you can assert when the last changes have been made (M-), when the last access has taken place (A-) and when the last file has been created (C-). If you can exclude that someone has manipulate the metadata that contain these time stamps the person who analyzes the data is in the position of reconstructing the last file accesses. If that is not the case it has to be searched for evidences that prove that someone has manipulated the metadata or file systems and in which way.

The file names and directory entries are possibly not available for reconstructed files. In this case the expert tries to find evidences 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 the pattern recognition searching method mentioned above. The disadvantage of this method is that you have to look manually at the each single picture. Very rarely a header of a file reveals additional information on its creator or source server. The stored data can be searched for special terms 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. (level 5 see figure 3).

Chapter 3

Client and Server Analysis

Depending on the kind of machine that should be investigated you can distinguish between client and server forensic. The former kind of forensic analysis is more appropriate when you are searching for evidences of the possession or the distribution of illegal data contents. In order to arrest a person who possess 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 pornographical photos of children) that was especially developed for this purpose. One of the disadvantages of this program is as follows: As the possession of this kind of pictures is liable to persecution it is not allowed that the software includes respective pictures in order to use it as a sample. Therefore this program cannot recognize forbidden graphical material per se but only material that is already known and classified on the basis of a digital check-sum- method.

Besides these lacks of the software you have to take into consideration that the computer of a user can be abused for exchanging this forbidden material without his knowledge via a security weakness 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 computer: This includes modem, DFÜ network connection and the connection to the internet and to the printer. It also takes into consideration the search for security weaknesses that could have been used by an intruder. Log files such as event log of NT or sys log of Unix are also useful. They contain several information that are relevant for the analysis. Among others: when and how often a user logs

on and off and at what time the PC was online and so on. A 65-year-old administration employee of an American university was dismissed as she had been accused of having stored pornographic pictures in her computer. The client-analysis brought it to light: As she had missed to log off her computer the cleaners could abuse her account for browsing the Internet. Analyzing the server can also help to take hold of the intruder as the following example shows: One morning an administrator found on the panel 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 retracing the attack. The log files and the 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 are also available it is possible to perform forensic accounting. Forensic accounting data possibly allow to track the source of the attack or the hacker as far as he or she had not used another hacked computer as starting point for his or her attacks.

Chapter 4

First Aid for Administrators

When you discover an attack on your system:

- keep calm and please do 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 with the exact point of time
- Please 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 oneself when you do not have technical knowledge but to contact an expert

At the actual scene of crime it is important to assert who has access to different rooms and computers or how access and execution rights are distributed within the company. In this way it is possible to restrict the number of suspects. As a last working step after the analysis of all data preparation of all gathered evidences 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 specialized is limited to technical evidences. How difficult it is to communicate this to the non-technicians that are involved in this process is proofed by the request for printing out the whole content of the hard disk that is quite often made by companies as the data securing company ibas reported. In case of a modern 80 GigaByte hard disk the printing would result in a mount of paper amounting to the heights of the Mount Everest.

Chapter 5

Translation of technical facts for technical laymen

The translation of technical facts into comprehensible examples is very time-consuming as reported by Thomas Schwarze, head of department forensic communication and information technology of the regional Criminal Investigation Department of Hamburg. The making of an expert opinion takes approximately as long as the actual investigation. Of little comfort is indeed: If there are clear evidences and it comes to legal proceedings, in general it is managed to translate the technical facts and the prosecution wins the case.

As attacks on computer systems cannot be eliminated completely despite precautions, administrators should take those steps in time that facilitate the forensic analysis. As a first move 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 exactly so called alerting chains, areas of responsibilities and the way of proceeding. Users should be sensitized for security subjects and be inducted into the company's security policy. As a next step the person who is responsible for the system should document the whole network with all active components. The 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 appliance such as an intrusion detection system or a firewall depending on the demand of security.

Chapter 6

Central collection of evidence

For subsequent retracing of incidents it is important to know when and what had happened. Each of the newer Microsoft operating systems (such as Win2k or XP), all derivatives of Unix, Novell Netware and Cisco IOS Software support the Network Time Protocol NTP (www.ntp.org). It serves as a basis for the installation of a time stamp 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). It is also advisable to operate a central log server. Due to secure procedure it collects all log messages from the network (server farm) and writes it down 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 of the single servers are correlated here. As a result it will be more difficult for an intruder to cover his tracks. In order to discover the spoofing of an operating system, such as by rootkits, the administrator of the system should create a list of MD5 checksums of all system binaries and the system core at a clean state of the system. In case of an attack you can compare the check sums to see which data have been changed. Even if the measurements mentioned above help to improve the securing of evidence in the worst case there can be obstacles. One of the difficulties that can occur are the different encodings of the stored data depending on the kind of operating system (ASCII under DOS, EBCDIC with IBM Mainframes, AS/400, Unicode under Linux, Windows 2k und XP). There is also the fact that there are still a large number of additional binary formats. If there

are picture and sound files on the system the number of binary formats is even larger. The analysis is hampered as well by encrypted data systems such as produced by program PGP disk. There are no guaranteed prospects of success. But in case of additional efforts even these data can be used. In order 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 in order to perform a forensic analysis further knowledge of operating and file system, networks as well as file formats and metadata is essential.

Chapter 7

Looking into a forensic specialist's 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 tries to determine the kind of file on the basis of the initial part of the file. Due to this command the analyst is in the position to analyze the image of hard disk that was cloned by using `dd` under unix. An image cloned by using TASK displays the following contents of the main directory:

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 in the position of cloning hard disks, performing analysis on the image as well as searching the database for images, documents and other patterns.

One special feature of EnCase allows you to search for file 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. Only by using a boot disk it can be started on a system without any additional installation.

CHAPTER 7. LOOKING INTO A FORENSIC SPECIALIST'S TOOL-BOX14

You can search for evidences 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.

Chapter 8

Interview with Thomas Schwarze

8.1 Forensic work of the police

An employee of a software company gave notice to his job and established a company of his own. Only shortly after that this company sells its own software that looks very similar to the software of the other company. Like a scene of a spy film? Far from it! This withdrawal of company secrets is one of the most common crimes that are investigated by the department forensic communication and information technology (abbreviated IuK = Forensische Kommunikations- und Informationstechnik) of the regional Criminal Investigation Department of Hamburg. The prospects of proving the withdrawal of company secrets are quite good, is reported by Thomas Schwarze, head of department. The offender often leaves a vast number of marks on their computers. Since mid-eighties all regional criminal investigation departments have found departments that focused on crimes that are 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 an expert opinion and legal action, are performed by experts. An ever increasing number of computer related crimes and the rapid development of technology, demands regular extension studies 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 a case in court. Sufficient funds for the increasing demand of staff and know-how is 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 one as well, a cloning of the hard disk of these systems is made on the spot. A more serious problem is the protection of data privacy: Sensitive data such as financial, medical and other data are 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 these data. An answer to this problem has not been found yet. Nothing else remains to be done as to rely on the obligation of secrecy of the officials.

Despite all difficulties Thomas Schwarze is quite satisfied with his team. Those cases that are submitted to a court are fought successfully due to the 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.