Towards Requirements for a Case Preparation Support System Based on Digital Evidence

M. Bielecki and G. Quirchmayr

University of Vienna, Faculty of Computer Science, Austria
e-mail: {Gerald.Quirchmayr, Maximilian.Bielecki}@univie.ac.at

Abstract

This paper describes an approach for presentation and argumentation support systems within a legal IT forensic case. The first part is dedicated to a very short analysis of the current legal situation in the context of Austrian laws and regulations. This analysis is followed by a discussion about gathering digital evidence, which provides the basis for the entire argumentation process. The paper then continues with the presentation of our approach towards developing an automated expert software tool for supporting the generation of an argumentation strategy needed for taking a case to court. The core aim of this paper is to demonstrate the need for a tool which is capable of preparing an IT forensic case based on the digital evidence provided by forensic specialists. The results have to be presented in an understandable way so that also people who are not specialised within this kind of forensics can understand the produced results and work with them.

Keywords

IT forensics, legal regulations, argumentation strategies, formal models, digital evidence, framework concept

1. Motivation and background

As surveys carried out over the past decade have shown, the number of computer crime incidents is constantly growing (AusCert, 2006; Richardson, 2008). Modern criminal organizations have started to focus their current activities on novel digital technologies and shifted their illegal actions into a new virtual area. Several different new forms of threats have therefore evolved and finally legal authorities have had to adapt to this new situation. New police departments were founded (which were mainly focused on computer crime cases), new laws were established and special investigations initiated. The main drawback behind this adaptation process was and still is that legal systems (especially procedural rules) in general remained untouched. Hackers, crackers and all kinds of digital criminals still have to stand up in court in front of a judge to finally get convicted. Technology in combination with these fundamental basics of executing the law has led to several new challenges. First of all, the question is how to catch people who commit a crime or an illegal action within a virtual world. This problem was addressed by introducing the novel analysis of IT forensics. Specialists were trained to identify what kind of computer crime happened, what actions were performed and most important who was responsible. This information can be gathered through specialised software tools such as EnCase (Guidance Software).

This situation clearly demands a tool supported, if not a fully automated, process to overcome these problems. Besides analysing the digital evidence, there is the need for a solution that generates results which can be used in a legal court case. Additionally, it has to provide a goal-driven argumentation strategy to verify the gathered digital evidence against.

One of the biggest positive side effects of an automated solution would be the increase of efficiency. Court cases could be finished in a much shorter period of time. There would be a much lower demand for highly skilled specialists who can verify and interpret the gained results in the right direction. Finally, this development would result in an approach to reduce additional costs of court cases which would not have to deal with highly technical knowledge anymore because the provided results would be presented in a way that also non-technical people could understand.

2. The Current Legal Framework in Austria

Before any formal models or any technical solutions can be discussed, an explicit border line has to be drawn. Within this paper only current Austrian regulations will be discussed and taken into consideration, because even the continental European diversity would go beyond the scope of this publication.

According to the Austrian criminal proceeding (“Strafprozessordnung”) during a court case there are several important steps which have to be taken into consideration (RIS, 1975). The first step is to identify the involved parties (“legal persons”) and the responsible court. There are several different types of courts in Austria which all have different authorities. Additionally, there is often the main problem to identify all involved people within a legal case, especially in computer crime cases. Very often it is extremely difficult to find the explicit offender, because novel techniques obstruct successful investigations.

The next important aspect for a successful court case is the law of evidence. The gathered evidence has to provide the necessary information to prove that a criminal act has occurred and who was responsible. Within computer crime cases it is often difficult to secure the evidence in an enduring way and avoid additional, mostly unintended, manipulation. One common approach for this problem is to confiscate and seal all involved technical devices. But in cases where entire server farms are involved, it is impossible to shut down the entire system and transfer it to an examination site. There clearly is a lack of a more effective way to deal with this problem. Besides the common problem of avoiding the manipulation of evidence, there must also be a closed chain of evidence. A detailed log has to be administrated to confirm what happened to all systems and data, who had access and could manipulate them or who could accidently have changed information.

Additionally, the law of evidence takes testimonies into account and even deals with automated data analysis (“Rasterfahndung”), monitoring of telecommunication networks and even optical and acoustic observation of potential criminals using technical devices (“Lauschangriff”). All these legal actions can be initiated as a matter to secure the crime scene for possible investigations.

The final criminal proceedings are based on two different investigations. First, there is a prelodgement before the entire case even gets to court. In Austria there is the possibility that the prelodgement is even initiated against an unknown offender. The aim is to identify all involved people within this case. As a next step, a preliminary hearing takes place to decide whether the investigated offenders can be sued or not. Only if this hearing ends successfully, a court case will be started.

The detailed steps during a court case are very similar to other European countries and will therefore not be discussed in detail here.

Another important note about the current legal situation in Austria is the constant evolution of classic computer crime legislation. In the early stages of computer crime legislation the main focus was on classical burglary or damage of property, such as the destruction of computers. With novel technological solutions and the broad acceptance of the Internet, a completely new area of computer crime incidents has evolved. That is why the legal regulations had to be adapted to these new circumstances. There were incidents where computers suddenly were misused by criminals and participated in global criminal acts. But who was responsible in the end? Is it possible to find the offenders or is it just the owner of the machine who is held liable? Legal systems had to deal with this new situation and new laws were enacted.

For instance, before 1987 the intentional deletion of computer software through a third party was not an illegal act in Austria, because the device which stored the program was not irrevocably destroyed. To solve this problem, the Austrian legislation enacted some new laws in 2002. New acts of crime were defined or modified within the Austrian criminal code (“Strafgesetzbuch - StGB”):

- The act of data corruption (§126a - “Datenbeschädigung”)
- The act of fraudulent data misuse (§148b - “betrügerische Datenverarbeitung”)
- The act of illegal access to computer systems (§118a - “Widerrechtlicher Zugriff auf ein Computersystem”)
- The act of violating the telecommunication law (§119 - “Verletzung des Telekommunikationsgeheimnisses”)
- The act of illegal eavesdropping (§119a - “Missbräuchliches Abfangen von Daten”)
- The act of manipulating a computer system (§126b – „Störung der Funktionsfähigkeit eines Computersystems“)
- The act of data misuse and illegal access (§126c - „Missbrauch von Computerprogrammen oder Zugangsdaten“)

- The act of falsification of data (§225a “Datenfälschung”)

It would go far beyond the scope of this publication to explain in detail all novel regulations which have evolved during the last years. The conclusion of this chapter is that the legal situation has been adapted to be able to deal with novel criminal incidents. New laws were enacted and now they have to be obeyed, which automatically leads to the next question: Who can ensure that the current laws are obeyed? Besides this fundamental question the general legal framework has been defined which can be used for current court cases.

3. Requirements for Digital Evidence as Basis for Case Preparation

As already stated in chapter 2, digital evidence marks the crucial part of a computer crime case. It is vital for the entire court case and has to be discussed in every detail.

First of all it is important to clarify that according to the current legislation all evidence must be handled in the same way. There is no difference in the type of cases. If digital evidence has to be collected, the same security controls have to apply for a civil lawsuit or as they do for a major crime case.

As a first step, digital evidence has to be identified at the crime scene. It can be any information stored or transmitted in any digital form. Due to the technological evolution, digital data can be found not only on obvious computer or server systems. Digital evidence is often stored in the following locations:

- Hardware
  - Mainboards
  - Hard drives
  - Ram modules
  - PCMCIA cards
  - Chip cards
  - Entire systems
- Client / Server / Middleware/ Host
  - Transaction servers
  - Backup devices
  - CCTV systems
  - Copying devices
  - Fax machines
- Access devices (especially log files)
  - Mobile phones
  - Music players
- Peripherals
  - Printer
  - Scanner
  - Phone systems (PBX)
  - Log files of dial numbers

- Mobile devices
  - PDAs
  - Mobile phones
- Date storage devices
  - Floppies
  - CDs /DVDs
  - Dongles
  - Pen drives
  - USB storage devices
- Client software
  - Email client
  - Office data
  - Internet browser
  - System logs
  - Dongles
- Server software
  - Services, Applications
  - Databases
  - Gateways
  - Domain Controllers
  - Log files

As computer data and digital evidence usually are very sensitive, it is important to classify the different types of data:

Volatile data

Volatile data is information that will be lost after a system shuts down. It contains cache values, logs of the current network connections, all running processes and information about logged users.

Fragile data

Fragile data contains information that is stored on a hard drive but changes its condition when it is accessed directly.

Temporary data

Temporary data persists of information stored on a hard drive that can only be accessed under special conditions like during the runtime of a program.

The process in which order the different data has to be collected and stored is described within the RFC3227 (The network group, 2002). Briefly speaking, it defines the order of volatility and suggests that digital data should be collected in the following order:

- Registers, cache

- Routing table, arpcache, processtable, kernel statistics, memory
- Temporary file systems
- Hard drives
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival and other external media

There are four main steps for collecting digital evidence in general (Nelson, 2006):

- Identify digital information that can be used as evidence.
- Collect, preserve and document all digital evidence.
- Analyse, identify and organize the gained evidence.
- Try to rebuild the evidence and re-enact the crime to verify that the results can be reproduced reliably.

The first three steps of his structured model are often referred to as **S-A-P** model. First **S**ecure the crime scene. Afterwards **A**nalyse the found evidence and as a last step **P**resent the gained results. Those three steps together define the S-A-P model.

According to the RFC3227 guidline every investigation of digital evidence has to follow a systematic approach (The network group, 2002). There must always be a detailed documentation of all processes and of all involved personnel to reduce the risk of losing evidence and to avoid confusion or damaged data.

Standard procedures require that digital data is secured and sealed in a way that subsequent obfuscation is impossible (The network group, 2002). Especially peripherals have to be taken into consideration because they can store important digital evidence as well. Besides securing data, digital evidence has to be catalogued for further investigations. Another aspect which is very important during an investigation is the storage of digital evidence. Modern computer systems (especially server systems) can contain several hard disks with several Terabytes of data. All this information and data has to be stored via bit-stream copies to independent systems to verify that data cannot be lost. Novel blu-ray drives can provide the needed space for read-only data. Additionally, modern RAID systems can be used as well to handle this huge amount of data.

One very important aspect for a successful digital data investigation is to obtain digital hash values from the collected digital evidence. Hash values are generated through mathematical algorithms that calculate exactly one output for a given input. The interesting part of hash values is that it is almost impossible to find any collisions with another input. The same input will always generate the same hash value. This function can be used to maintain data integrity and to confirm that the stored data was not manipulated or changed. The most common and widely used hash algorithm is MD5 (Message-Digest algorithm 5 found by Ron Rivest).

4. Envisaged Approach Guided by the Identified Requirements

As already discussed in the two previous chapters, the Austrian environment has been adapted to the novel digital crime scene with new laws and regulations. Besides the legal situation, the process of collecting digital evidence was described and discussed within the last chapter. Based on this background, we can now introduce our approach to introducing a framework model which will be the basis for developing argumentation strategies. This argumentation strategy is needed to effectively support lawyers during a computer crime court case with technological assistance. It should provide a detailed analysis and documentation of what exactly happened, who was the offender and who was the victim of the crime. The main idea behind this approach is to create useful interpretations in a form that also non-technical people can understand the results produced by a forensic investigation.

To achieve this goal, a general framework has to be established to evaluate the gathered results and structure the ensuing argumentation strategy.

The following framework model describes a very general approach to structure possible attempts with the help of a modern forensic software tool, in our example EnCase. EnCase is an industry standard software tool specialised for computer forensics. It is capable of sealing digital evidence, storing and documenting digital data and analysing every single bit of information (Guidance Software).

To create a successful argumentation strategy, there must first be a conclusive analysis of the secured digital evidence. The first step to analyse provided data is to get the current system time of a system. The system date is crucial too for the timeline of possible criminal acts. Afterwards, the entire memory of a system (located within the RAM) has to be stored and analysed. Malicious software can often be located within this area for two reasons. First, this kind of memory only stores volatile data and second, it is difficult to obtain and often forgotten. As a next step all running processes have to be archived and verified. If a system was compromised, all process could be hostile and should not be treated as trustworthy. It is important to verify the functionality of all processes. Special system processes are sometimes difficult to verify because due to the lack of open source codes some processes are not well documented and the functionality is not clear. Besides the running processes, the logged and current users have to be checked. Sometimes criminal offenders try to manipulate user accounts to gain additional rights and permissions. In addition, all network connections have to be checked. Afterwards all logs have to be verified and analysed to get a hint on how an offender could get access to the system. As next and very important step timestamps of all data files have to be generated because they can help during an investigation to find all data which was manipulated or changed. It is important to consider that the actual timestamps provided by a compromised system can be forged or manipulated. Another good attempt to analyse what exactly happened to the system is to investigate the remaining swap file. It can contain additional information which is often already destroyed or manipulated. Afterwards all drivers loaded into the operating system have to be checked and verified. All of them have to be documented and tested to confirm that no malicious software is masquerading as a running driver. Another good place for useful information is the registry of an operating system. It stores all crucial system parameters and is mandatory for the operating system. If something was manipulated within the registry, the entire system will be influenced. As one of the last steps the system event log has to be investigated. In most cases this is actually the first place where criminals try to masquerade their activities by blocking or deleting the log files. Nevertheless, it has to be taken into consideration because it can provide helpful hints. Additionally, the command history has to be checked as well and all current user group policies. Finally, one more place to look at should be the user's clipboard. Sometimes malicious software hides the needed data within the clipboard system to avoid any detection.

For more detailed information on this standardized process, the reader is referred to the RFC3227 guideline (The network group, 2002).

Based on the evidence gained during the investigation process, as already mentioned above, the concluding argumentation strategy has to be created with the help of an additional software tool (which has to be developed).

Figure 1 shows an overview of possible threat scenarios and the related analysis. If during an investigation suspicious network transmissions are detected, the investigator has to focus on what kind of transmission was initiated, who was the other party, how the other party managed to get access to the system and who is finally responsible.

The whole process runs differently if an access violation could be identified during the analysis of a compromised system. In such a situation, the investigators have to spot the malicious user profile that was used to gain access. Besides all, access and user logs have to be checked to find any manipulated data.

As already identified, the main crime related to computer systems can be described as data manipulation, which also includes data deletion, data manipulation or data falsification. In this context EnCase proves to be a very efficient software tool which is capable of easily extracting manipulated data within a compromised system. For a successful court case this digital evidence of manipulated data is still of only limited use. The right explanation and especially presentation is necessary to prepare all gained results with the focus on an upcoming court case.

Therefore there is an urgent need for a support system which is capable of taking all results evaluated by EnCase (for instance) and generates digital evidence in a simple language so that also non-technical people can understand it. This is crucial for the success of our approach. The presentation of the evidence and the entire computer crime has to be more or less self-explanatory to finally help a judge or a jury to understand the whole criminal act.

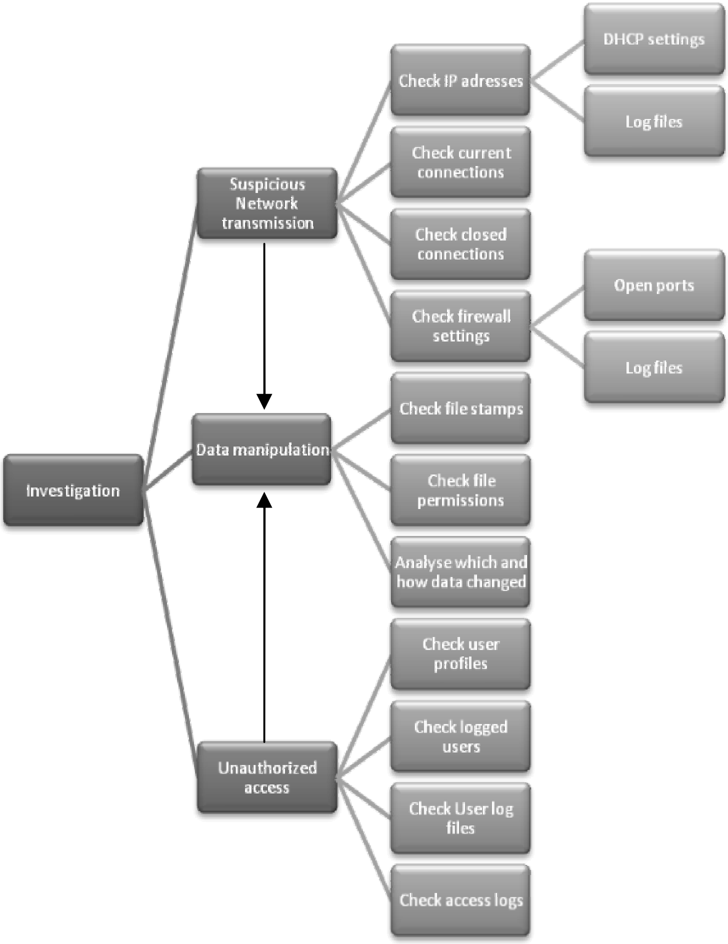

Figure 1: Decision tree for possible threat scenarios

It is obvious that such a support system has to be built on a modular system core to guarantee the possibility of constant updates. Additionally, there must be an easy way to implement and add new argumentation strategies which have to obey the newest laws and regulations. Besides this, the system needs to provide the following functionalities:

- Well documented and described analysis
- Understandable and efficient GUI
- Interfaces to deal with different inputs (frum systems like EnCase or FTK)
- Comprehensive reporting tool with output generation
- Adjustable presentation settings

5. Conclusion

As discussed in this paper the legal situation has already been adapted to the new threats that are existent in the global networked world. Computer crime is still constantly evolving and threatening every networked computer system. It is difficult for law enforcement and prosecution to remain one step ahead because of bureaucracy and procedural regulations and limitations. Nevertheless, the legal framework has already been adjusted (in Austria as described in chapter 2) into the right direction, but there is still no efficient way to deal with the problem as a whole.

One other very important aspect which is closely related to computer crimes and especially to computer forensics is the collection and handling of digital evidence. Digital evidence of a computer crime can be found in almost any digital device. It is no longer limited to computer or server systems. Due to the fact that modern MP3 players and mobile phones often have sufficient computing storage and power, they can keep information that can be crucial for the entire court case. It is very important to remember that digital evidence which is gathered during an investigation has to be well documented and must always be approached in a systematic way. This process guarantees a neutral and objective investigation which can be very helpful during a court case. Besides sealing typical hard drives, it should be taken into consideration that computer systems do not only include hard drives. All connected peripherals have to be investigated as well because they can provide additional information. Besides attached devices it is also very important to understand the different volatility levels of data which all have to be handled in a different way.

Based on the legal regulations and the described investigation of digital evidence it is obvious that there is a need for a support system that is capable of presenting the gained results in an understandable way. First the system analyses the provided results from a forensic tool and afterwards it reconstructs the possible computer crime. In the final step of the process this system generates an argumentation strategy that can be used in a court case and increases the efficiency of court procedures by linking the argumentation directly to evidence that is presented in an understandable way.

The main aim of this paper was to focus on the requirements to provide the needed framework for possible further developments. The current legal and technical situations were discussed to demonstrate the need of a support system which is capable to provide lawyers and judges with appropriate technical evidence.

Besides that, the goal of this paper is to point to a way for increasing the efficiency of legal court cases. The evidence gathered at the crime scene (in this case on the computer system) and the results gained through forensic tools still do not provide the level of presentation which is needed in court. There is still a lack of an appropriate system that can fully automate the interpretation of existing results.

6. References

AusCert. 2006. Australian Computer Emergency Response Team. [Online] 05 2006. [Cited: 20 01 2009.] http://www.auscert.org.au/images/ACCSS2006.pdf.

Guidance Software. EnCase Forensic. [Online] Guidance Software.[Cited: 02 01 2009.] http://www.guidancesoftware.com/products/ef_index.asp.

Nelson B., Phillips A., Enfinger F., Steuart C. 2006. *Guide to computer forensics and investigations* . Boston, USA : Course Technology, 2006.

Richardson, R. 2008. CSI Computer Crime and Security Survey 2008. [Online] 07 10 2008. [Cited: 20 01 2009.] http://www.gocsi.com/forms/csi_survey.jhtml.

(RIS), Rechtsinformationssystem des Bundes. 1975. Rechtsinformationssystem des Bundes (RIS). *Strafprozeßordnung 1975*. [Online] 1975. [Cited: 20 01 2009.] http://www.ris2.bka.gv.at/Dokumente/Bundesnormen/NOR30006190/NOR30006190.pdf.

Sammes, T. and Jenkinson, B. 2007. *Forensic Computing*. Swindon, UK : Springer, 2007.

Schmölzer, G. 2003. *Informatikrecht.* Österreich : Springers Kurzlehrbücher der Rechtswissenschaft, 2003.

The network group. 2002. RFC3227 - Guidelines for Evidence Collection and Archiving. [Online] 2002. [Cited: 16 01 2009.] http://www.faqs.org/rfcs/rfc3227.html.