Digital Forensics in Computer and Cellular Networks

Pascal Schöttle

July 19, 2009

Seminararbeit
Ruhr-Universität Bochum

Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Abstract

The goal of this paper is to give an introduction to the field of digital forensics (also known as computer forensics) in computer and cellular networks.

Due to the fact that the number of crimes done with electronic devices such as computers or cell phones is increasing the need for more research in this area of investigation is obvious. Even classical crimes like fraud or money laundering leave electronic traces and to safe these traces can hold good evidence against criminals. Instead of classic investigation, which has a long history and good predefined methods, computer crime investigation is a relatively new science with a lot of different approaches and frameworks.

First of all the term *digital forensic* and its use in nowadays science will be explained. The terms digital evidence and digital investigations are introduced.

Digital forensics is the main part of computer crime investigation and the question that rises is what kind of information can be used to prove someones guilt. What kind of traces of a possible attacker holds against him and how it can be proved that this data was not changed since the attack.

The problem here is clear when considering cases in courtroom. You can not blame someone a crime with speculations and unproven facts. Furthermore you do not want the alleged criminal to argue that maybe the data you are using against him could have been altered.

This questions and problems arise in computer and cellular networks as well and are topic of actual discussions.

To fully understand where and why criminals or suspected criminals leave traces in networks, this paper gives a short introduction to widespread network technologies before demonstrating how forensic methods can be applied to networks in general first and later specialized with different network protocols and layers of the OSI reference model respectively.

Contents

1 Introduction

The goal of this section is to introduce the terms *Computer Crime*, *Digital Evidence* and *Digital Forensic Analysis* and show their basic concepts.
There are two aspects of *Computer Crime*, which are defined by the worlds leading computer forensic equipment company DIBS [DIB] as follows:

- *A criminal act in which a computer is essential to the perpetration of the crime.*
- *A criminal act where a computer, non-essential to perpetration of the crime, acts as a store of information, concerning the crime.*

This is to say that not only the crimes committed directly with a computer belong to this field of offense but also crimes where evidence could be found on computers or networks without necessarily using those devices to actually commit the crime.

> **CASE EXAMPLE**
> If the police has a certain suspect in a homicide, the investigation of his computer may reveal certain details about his contact to the victim (e.g. emails and chats), or even research about how to get rid of a corpse. The analysis of the suspects cell phone may refute his alibi or also give details about contact between suspect and victim.

With this definition it becomes obvious which important role digital crime analysis has nowadays and that its role in crime investigation will not decrease but more likely increase in the oncoming years.
There is nearly no imaginable crime in which no computer or network can be involved. Therefor, besides the increasing number of electronic fraud or crimes committed directly with a computer, the branch of digital investigation will become more important for classical evidence collection and crime investigation.

The term *Digital Evidence* describes all the information that can be gained from electronic devices. This can be storage media like hard disks, network logs, cell phone logs, emails and so on.
One of the main problems of Digital Evidences is that most of them are volatile and there is always a possibility for the perpetrator to erase them. Due to this

Figure 1.1: The three major phases of digital investigation according to [Car05]

fact, the time within which the evidences are secured is more important in Digital Investigation than it might be in classic investigation.

Digital Forensic Analysis is divided into two main branches. The first one is *Physical Storage Media Analysis* and the second *Network Analysis*. This paper focuses on the second branch. However, the two branches cannot be separated completely, so there will always be comments about looking on storage media for evidences which support or refute a hypothesis made.
One of the standard works on Digital Forensic Analysis is Brian Carrier´s *File System Forensic Analysis* [Car05]. Although, as the title indicates, its main aspect is the File System there are some basic ideas that can be applied to Network Forensics as well. In Figure 1.1 the three major phases, as indicated in [Car05], can be seen. These are the *System Preservation-*, *Evidence Searching-* and *Event Reconstruction* Phase. As Figure 1.1 indicates these three phases do not need to occur one after another but there are trackbacks from every phase to the previous.

1.1 System Preservation

This phase is always the first thing to do once a digital crime is detected or even assumed. As with classic crimes the first act of investigation is to preserve the crime scene. This is the main aspect of this phase. In classic crime investigation you can close of the crime scene, e.g. a house or flat, but it is more difficult to follow this approach in digital investigation. Here it is difficult to shut down a network or computers without altering data. As with classic crime scenes it should be tried to avoid every change of the evidences. It has to be tried to copy and save all informations contained in the network or on physical storage devices without changing them. It is important to have a proof that the data was not changed during the investigation process. One approach to achieve this is to compute a cryptographic hash sum of the data, which would indicate a change of them later.

1.2 Search for Evidence

Now, after the crime scene is preserved, the next step is to look for evidences. As a digital crime is assumed the digital investigator creates hypotheses which can either be supported or refuted by evidence found in the data. It is a major aspect not only to look for evidence that supports a specific hypothesis because the hypothesis always could be wrong. The main methods for searching for evidence are:

- to look at log files, e.g., those of routers or other network components,
- search for altered data, e.g., again with cryptographic hash sums,
- looking for root kits, e.g., by checking the low levels of the operating system,
- search the file system for ominous files.

CASE EXAMPLE from [Car05]
Consider a server that has been compromised. We start an investigation to determine how it occurred and who did it. During the investigation, we find data that were created by events related to the incident. We recover deleted log entries from the server, find attack tools being installed on the server, and numerous vulnerabilities that existed on the server. Using this data, we develop hypotheses about which vulnerability the attacker used to gain access and what he did afterwards. Later, we examine the firewall configuration and logs and determine that some of the scenarios in our hypotheses are impossible because that type of network traffic could not have existed, and we do not find the necessary log entries. Therefore, we have found evidence that refutes one or more hypotheses.

1.3 Event Reconstruction

The third and last phase of the digital investigation process is to use the collected evidences to reconstruct what has happened in the system or network. To do this, it is necessary to correlate various evidence, maybe even from different sources, to get a proof of the one hypothesis that stands last. For this phase it is important to have a knowledge of the operating systems and the network basics of the digital components involved in the crime. To understand how an operating system or the network components work is essential to come to a clue what the hints are indicating.

1.4 Summary and Outlook

In summary, the procedure of investigating a digital crime is very similar to the procedure of investigating a classic crime. First of all, there is the crime scene which has to be preserved. Than, there is the search for evidence and finally the result of this search is to reconstruct the events happened at the crime scene. The main difference is the problem of time. In digital networks as well as on stand-alone systems, the danger of data being altered is more likely than with classical crimes. Usually the perpetrator has to undertake own actions to dispose most of his traces on a classical crime scene whereas in digital crime scenes the traces and evidences are often automatically overwritten by the overlying system after some time. So, if the recognition of a crime takes very long or the preservation of the crime scene is not done right away, there is a good chance for the perpetrator that his traces are gone altered, deleted and thus not useful anymore. Due to this, the first act of every digital investigation has to be to preserve evidences as fast as possible.

To fully understand where the traces an attacker may leave are, the investigator has to understand the crime scene. For this, Chapter 2 gives a short overview over network technologies. Chapter 3 shows how forensic methods can be applied to networks in general and Chapter 4 applies methods directly to the different layers of a network. Chapter 5 concludes this paper.

2 Network Basics

As mentioned in Section 1.3, it is indispensable for a digital investigator to know the field he is investigating in. Hence, it is necessary to give a little background on how digital networks work to review the most important network protocols.

2.1 The most widespread network technologies

As it can be seen in Figure 2.1, there are many interfaces and protocols through which Local Area Networks (LANs) can communicate with each other. Nowadays, almost every LAN is connected to the Internet where the definite standard is the TCP/IP language. Due to the fact that the first step of a digital crime investigation is to look for traces in the LAN before extending the search to the Internet, here is a short overview on the most widespread technologies for LANs.

Figure 2.1: Dissimilar Networks connected via Internet (see [Cas04])

2.1.1 Ethernet

After several stages of development Ethernet is the most widespread technology used in private and corporate LANs. It uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to coordinate communication of the different

hosts in a network. CSMA/CD is a "listen before acting" access control. This means that every host which wants to communicate over the shared network resource first listens to check that the resource (e.g. networking cable) is not occupied by another host and only sends data if the resource is available.
There are a lot of standards for different Ethernet- Revisions, which all have different purposes. The most widespread are 100BaseT and 1000BaseT because they are very cheap and easy to install.

2.1.2 IEEE 802.11 (Wireless)

The IEEE 802.11 standard summarizes various standards for Wireless LANs (WLAN). In these standards, the hosts, which do not necessarily have to be computers but also cell phones or PDAs, communicate with the Wireless Access Point (AP) using radio signals. Those APs are connected either to a wired network, e.g., an Ethernet, or directly to the Internet. The limitations of 802.11 in contrast to the wired networks are distance, speed and interference. There will be problems with the connectivity if a host is not within a certain distance of an AP or if there is a barrier between the host and the AP that blocks radio waves.

2.1.3 Cellular Networks

To overcome the limitations mentioned in the previous section, the use of cellular networks for data communication becomes more widespread and more available. For this, the cellular networks, which were originally intended to establish phone-to-phone connections for telephone calls, now operate more and more as packet-switched networks to connect to the Internet or even directly to LANs. But like with the connections build for telephone calls, the packet-switched connection makes the cellular phone or the PDA to connect to a cell site which is connected to the Internet and is responsible for routing the connections and the packets. Those cell sites keep logs which are used, e.g., for billing and maintenance but are also a good source for digital investigation.

2.2 Connecting Networks

Due to the various technologies mentioned in Section 2.1 and the different ways those technologies work, they can not communicate directly with each other. To enable this, the Internet protocol has been introduced to provided a common language for the LANs to communicate with each other. The most common Internet protocols are the Transport Control Protocol (TCP), the User Datagram Protocol (UDP) and the Internet Protocol (IP). Together (with a few supporting protocols) they are known as the TCP/IP internet protocol suite and are the *de facto* standard for nowadays communication on the Internet.

For a better understanding of TCP/IP and consequential a better idea where to find evidences in digital investigation and digital forensics respectively, it helps to look at the different layers defined in the Open Standard Interconnection (OSI) reference model (Figure 2.2). In this model there are different layers defined and each layer can contain informations, traces and evidences.

Figure 2.2: A simplified description of the Open System Interconnection (OSI) layers (see [Cas04])

As it can be seen in Figure 2.3, different applications can be reduced to first TCP or UDP and then to IP. This paper is too short to go into the details of all the layers but an example of how a web browser accesses the Internet, seen with the layers of the OSI model can be seen in Figure 2.4. Network tools (see Chapter 4), that intercept network traffic, can capture all the information that come from each layer and all of these informations can be good evidence for digital forensic.

2.3 Summary

It is essential for digital investigation and digital forensic analysis to understand the basics of nowadays networks. The differentiation between local area networks and wide area networks, mainly the Internet, is very important and also to understand the interfaces between those two. The following sections describe how the evidence can be found within the different network technologies presented in this section.

Figure 2.3: The different protocols in the OSI reference model (see [Cas04]).

Figure 2.4: A Web browser‘s access explained by the OSI model (according to [Cas04]).

3 General Forensic in Networks

As with classical crime scenes, a computer network can contain evidence that indicates that a crime has been committed, shows how a crime was committed, prove or refute hypotheses made by the investigator and disprove or support statements made by witnesses. A good example for the last point are cellular networks, where records are kept, when and where a cell phone was used. With this information the statement of a suspect person where he or she was at a certain time can be proved or disproved.

Unlike searching hard drives for evidence, which is relativly well-defined for the different file systems, there arise a lot more problems with searching networks for evidence. Hard drives are permanent storage media where the data can be recovered even if it was deleted. Networks are much more volatile and it is difficult to reconstruct a former state of the network in particular when a large number of different systems are involved.

Another big difference is that a hard drive can be analyzed offline but shutting down a network will destroy most of the digital evidence.

Furthermore, it is very likely that more than one network contain digital evidence for a crime. This first looks like a problem because there is more than one network which has to be analyzed. But it can also be an advantage because it is harder for the criminal to destroy all the evidence distributed over these networks.

As described in Chapter 1, the search for digital evidence is separated in different phases.

3.1 Preparation, Identification and Preservation

As mentioned above it is likely that not only one network is involved in a committed crime. So the first step of a digital investigation within networks is to determine which networks are involved in the crime. If those networks are identified, the next step is to contact the persons responsible for this network, e.g., an administrator of a company network. Many administrators collect data routinely to detect performance or security risks and these data can be a good source of evidence.

Also the Internet can be a source of evidence concerning emails and online platforms such as chats. Here, the digital investigators can contact service providers and ask for information when and maybe from where (with which IP address) a suspect has logged in the last time. Email providers even may give the investigators access to the emails sent by a suspect person‘s email account (of course only with permission of a court, otherwise the research in the email account of a suspect may be an offense by itself).

> **CASE EXAMPLE (BACH v. MINNESOTA 2002) see [BAC]**
> Accused of possessing child pornography, Bach argued that his Fourth Amendment rights were violated because a law enforcement officer was not present when his Internet Service Provider (Yahoo!) collected information relating to his account on their system. Initially, the district court agreed that the warrant was executed outside the presence of a police officer when Yahoo! employees seized e-mail from Yahoo!'s servers in violation of 18 U.S.C. 3105 and sections 626.13 and 626A.06 of the Minnesota Statutes, and thus the Fourth Amendment.

The identification process may be separated in several steps like when the suspect used the Internet to commit the crime his IP address may be logged but now the ISP, which holds this address, must be asked which subscriber had this IP address at the given time. In case the subscriber is another network, the logs of this network have to be examined as well.

Here, it must be considered that every computer has a network interface card (NIC) which is connected to the physical (or wireless) medium and which has a worldwide-unique MAC address. So sometimes it is more effective to filter data for MAC addresses rather than for IP addresses. But with enough knowledge of networks an attacker may fake his MAC address as well. So it is advisable to search for a combination of IP address and MAC address.

Sometimes it is helpful for the investigators to draw a so called *digital evidence map* displaying all the participating networks. An example of a digital network map can be seen in Figure 3.1. In this map the different Servers of a network with the particular operating system should be listed, as well as the access points to the network. The location of the entry points into a networks and the key servers often leads to the richest source of digital evidence.

Having identified all participating networks and entities, it is time for preserving data and log files. As mentioned above, routinely collected data can be a good source of evidence. Log files of network components(e.g., routers) can also provide good indication of what happened at what time in a network. It is very important to save this data before it is overwritten, again, time is a crucial factor. As mentioned in Section 1.1 it is very important to be able to prove later that the data collected was not changed during the investigation, so it is advisable to calculate a cryptographic hash sum(e.g., using SHA-1) of the collected data before starting to analyze them.

The International Association of Computer Investigative Specialists (see [IAC]) defines three rules for competent forensic examination:

Figure 3.1: Example of a digital evidence map (see [Cas04])

- *Forensically sterile* examination media must be used. *Forensically sterile* means that all media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.
- The examination must maintain the integrity of the original media.
- Printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted.

According to [Moh03] the first step in the preparation process is to generate an authenticated copy of all data found, the so called master copy, and then make another copy to process with. By this, it is possible to work with the data without running the risk to change it irreversibly.

3.2 Filtering and Evidence Recovery

Before searching the preserved data for evidence it is helpful to filter it for certain aspects. In most cases the amount of preserved data is very large and a lot of these data is not useful for the digital investigation. For example, if the whole traffic of a network is captured but there is only one suspect host in the network, all data which are in no way connected with this host can be removed, e.g., by the IP or MAC address of the host. Then the data related to this one host can be examined more closely for evidence it may contain. If this reveals a link to other hosts in the network, the filtering process has to be done again. But due to the master copy mentioned in the last section it is no problem to filter the data more than once.

The same applies for time periods. If an attack is suspected in a defined period of time, all data beyond this period can be eliminated.

Having reduced the data, the next step is to find evidence related to the suspect. First of all, the preserved and filtered data can be searched for suspicious network traffic which may support the assumptions made after the recognition of the crime. But if the suspected attacker is experienced and knows where he leaves traces, he tries to cover his tracks by deleting logs on network components or systems. Here comes the part of digital network forensic which overlaps with digital file forensic. All these data were on physical storage media and recovering data is often possible with knowledge of the underlying file system. In particular, the fact that a suspect has deleted log files on a system involved in an attack supports the hypothesis of his guilt.

3.3 Reconstruction Phase

As mentioned in Section 1.3, the main part of this last phase is to try to correlate the different evidences and thus reconstruct what has happened. For example, while investigating a computer intrusion, the first focus is on the attacker‘s IP address to determine which hosts were under attack. Then, the log files of these hosts can be compared for similarities in order to get a clue what the attacker tried and what he accomplished.

However, this phase of digital network forensic is more difficult than in digital file forensic because an attacker can be at several places, using different IP addresses at the same time, for example in a Distributed Denial of Service attack. Or he can cover his tracks by connecting to different computers all over the world before launching his attack from one of these computers. Therefore, it is necessary not always to believe the obvious but to question every evidence again to be sure it is no bait the attacker left purposely.

Figure 3.2 shows how an attacker hides his real location in California by connecting first via VPN to a server in Connecticut and then sending emails from there. To track down the attacker‘s real location, an investigator first has to find the origin of the email (in this case the server in California), then trace back the connection to Connecticut and from there try to find the origin of the VPN, again to California.

Figure 3.2: Example how an attacker fakes the origin of an email

3.4 Summary

Applying forensic technologies to networks is separated in different phases. It is not easy to shut a network down so that it can be examined offline. Due to this, time is an even more crucial factor in forensic network analysis than it is in file system analysis an classical forensic analysis. Many evidences on network components (e.g. routers or firewalls) are overwritten periodical just because of the limited resources those components have. If they are finally overwritten, this source of evidence is mostly lost forever, because it is not only deleted but overwritten, which makes it almost impossible to recover the data.

Another difference in network forensic is that there may be more sources of digital evidence which have to be correlated. This is due to the fact that an attacker can attack from several places in the network at the same time and thus leaves traces in more than one place.

4 Forensic Applied to Computer and Cellular networks

As seen in Section 2.1, there is more than one language for computers to communicate. The goal of this section is to show details where forensic methods can be applied within the different protocols or layers.

4.1 Ethernet - Data-link and physical layer

Applying forensic methods on the physical and data-link layer (as seen in Figure 2.2) is done by eavesdropping bit streams with tools called monitoring tools or sniffers. The most common tool on this layer are Wireshark (formerly known as Ethereal), which can be found at [WIR] and Tcpdump, which can be found at [TCP]. They both collect all data on this layer and allow the user to filter for different events. With both tools websites, email attachments and more that has been transmitted over the network can be reconstructed. An advantage of collecting this data is that it is directly connected to a host. If, for example the IP address or the MAC address of a host at a certain time is known, all data for or from this IP or MAC address can be filtered.
To establish the connection between IP and MAC address, it is useful to take a closer look at auxiliary network protocols. The Address Resolution Protocol (ARP) tables list the MAC addresses with the corresponding IP addresses.
To collect data on this layer, network interface cards (NIC) of a host can be put into "promiscuous mode". By this, they collect all traffic that comes over the network not only the traffic meant for this special host.
However, if an intruder or attacker is aware that his connection might be eavesdropped, he might use encryption to secure his connection. It is almost impossible to break nowadays encryption but the fact that a suspect‘s connection to another host is all the time encrypted might indicate that the other host is an accomplice of the suspect.

Besides raw data for sessions reconstruction, data collection on this layer has another gain. If examining higher layers and being in doubt of how accurate the assumption made are, e.g. whether log files have been altered or not, the data captured on this layer can either corroborate or debilitate the assumptions.
The big disadvantage of data collection here is that it will result in very large log

files to collect every piece of data. But because disk space becomes cheaper and the important data, like ARP tables, are volatile, more and more companies send at least a part of these logs to a remote storage medium where they are kept a longer time than they would be stored on the network devices.

4.2 TCP/IP - Transport and network layer

On the network layer the Internet Protocol (IP) is responsible for directing the packets generated by TCP through the network (e.g., the Internet) by adding source and destination information which can be interpreted by routers all over the network. Cellular digital packet networks, like GPRS, use similar protocols like IP, so the methods described for IP work with them as well.
For the correct routing, every intermediate router must have a routing table to know where to send the packet next. These routing tables are one of the best sources of information if investigating a digital crime and trying to track down an attacker. To do this, it is necessary to follow the packets of the attacker, reverse the sending route and find the computer the packet came from (i.e., the attacker).

Another source of evidence on this layer are authentication logs. They show which account and which user was associated with an activity and may reveal who was the attacker or at least sets limits to the people who come into consideration of being the attacker.

There are other kinds of logs like application logs, operating system logs or network device logs which all keep record of activities on a system. Of special interest are the logs of network devices because they provide an overview over network activities which is much more detailed than other logs. They can either be used to correlate events recorded by logs from other sources or stand alone as evidence for activities which were made during an attack. As with all network components they have limited storage resources and so many companies have configured their network components to send their logs to other servers to store them for a predefined time period.

4.3 The Internet

Sometimes the Internet is equalized with the World Wide Web (WWW), which is not quite right. A part of the Internet is the WWW but also services such as Email, Newsgroups, Synchronous Chat networks and Peer-to-Peer (P2P) networks are part of the Internet. Every one of these categories can be a rich source of digital evidence. The Internet is the one part of digital investigation which not only provides evidence of offenses made directly with computers but almost every offense made nowadays may leave traces in the Internet.

4.3.1 The World Wide Web

Since 1991 when the Web first became publicly available it has become more and more popular. Web servers logs can indicate that a suspect collected information which he needed for committing a crime and so they can indicate that this person really was the one who committed the crime.
Logs of a suspect‘s web browser can also either ratify or falsify statements made by him.

4.3.2 Email

A suspect‘s or victim‘s emails can also provide good evidence of a crime. But it is not always possible to prove that the owner of an email account was the one who sent the incriminating email. It is too easy to change the sender field of an email header to take it as a definite evidence. To prove that an email has really been send by a suspect the investigative methods mentioned in the earlier sections of this chapter have to be executed as well. But the email headers are a good indication in which direction the investigations should be deepened.

4.3.3 Other Networks

Like mentioned above every activity on the Internet leaves traces. If it becomes clear from a suspect‘s computer that he was active in chats or P2P networks, the logs of the applications should be reviewed to find out with whom he was in contact. This also includes the search on his computers for logs that the suspect may have deleted on his computer. It depends on the crime suspected if this procedure seems adequate(e.g., it would be justifiable in the case of a homicide but not in the case of fraud).

4.4 Positioning in Cellular Networks

Every cell phone has a Subscriber Identity Module, the so called SIM card. The SIM card contains the International Mobile Subscriber Identity (IMSI) which is a worldwide unique number. The IMSI is sent by the phone to the cell towers in its area to identify the phone, so that the calls for that phone are redirected to this cell tower and then to the phone itself. By the connection of the phone to a special cell tower a rough guess where the phone is located can be made. Because the cell phones try to get the best cell tower in their coverage, they search continuously for the cell tower with the strongest signal. To do this they send distance information with their request and if the distances of two, three or more cell towers are compared the guess about the position of the cell phone gets more and more precise. The accuracy of positioning depends on the concentration of cell towers in the area the suspect is. If he is in an area with a lot of cell towers (e.g., a city) the distances between his cell phone and the single cell towers are less and so the accuracy rises. If the suspect is somewhere in the landscape, where there may be only one cell tower in the range of his cell phone, the only thing that can be said about his position is that he is in this certain distance of this cell tower. Figure 4.1 shows how a phone can be located relative exactly using the information of three different cell towers. This determination of a suspects cell phone is a good information for digital investigators and can be used to prove or disprove a suspects alibi.

Figure 4.1: Example of how a cell phone can be located with three cell towers
Source: `http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790`

4.5 Summary

The goal of this section was to demonstrate that evidence occur on every network layer and that the layers cannot be considered separated. The first indication of a crime or an attack may occur on the application layer(e.g. somewhere in the Internet) but it is necessary to follow this indication down to the transport, network, data-link or even physical layer to get definite proofs of someones guilt or innocence. To do all this in an adequate period of time, it is advisable for digital investigators to have a knowledge about how data is send over networks so they know where there have to be traces of the activities. And if there are no traces they may have to admit that their hypothesis was wrong.

5 Conclusion

This paper gives a short introduction to the field of digital forensics. The main aspect here was the branch of digital investigation which deal with the traces and evidences that can be found in computer or cellular networks.
The main sources of this paper were the books about digital forensic by Brian Carrier ([Car05]) and by Eoghan Casey ([Cas04]). The scope of these books is much bigger and they both cover the field of file system analysis as well.
This paper shows, that an attacker or perpetrator who uses digital networks, inevitably leaves traces within them.
As the Internet and all other networks can be divided into different layers, as defined in the OSI reference model, an investigator in this field has to know the basic functions of these layers and has to know how to correlate evidences found on different layers.
Another essential attribute of evidences found in digital networks is that they are often much more volatile than in classical crime scenes. Due to this, the first goal of a digital forensic analysis is to be as fast as possible with collecting data and preserving the crime scene.
The main conclusion of the paper is that investigating a digital crime within networks is not completely different from investigating a classical crime. The first step with both is to preserve the crime scene, then comes the search for evidences and in the end conclusions have to be made by reconstructing the events.

The big difference with digital investigation is that there is no standardized modus operandi and it is not always clear how courts judge the correctness and the significance of the evidences collected.

In [Ste08] Stein demands a standardized routine for common cases, a catalogue of action for difficult cases and an agreement on how digital forensic reports have to be structured. It would make the field of digital investigation and forensic much easier if these things would be realized.

List of Figures

Bibliography

[BAC] http://epic.org/privacy/bach/. Bach v. Minnesotta (2002) Appeals Court, 8th Circuit, Case number 02-1238.

[Car05] Brian Carrier. *File System Forensic Analysis.* Addison-Wesley Professional, 2005.

[Cas04] Eoghan Casey. *Digital Evidence and Computer Crime.* Academic Press, Inc., Orlando, FL, USA, 2004.

[DIB] http://www.dibsusa.com/methodology/methodology.asp#1. Disk Image Backup Systems - DIBS USA Inc.

[IAC] http://www.iacis.com/. The International Association of Computer Investigative Specialists - IACIS.

[Moh03] George Mohay. *Computer and Intrusion Forensics.* Artech House Inc, Norwood, USA, 2003.

[Ste08] Stefan Stein. *Computer Forensics - Sicherung und Analyse von forensischen Beweisen im IT-Umfeld.* VDM Verlag Dr. Müller, Saarbrücken, Germany, 2008.

[TCP] http://www.tcpdump.org/. TCPdump.

[WIR] http://www.wireshark.org/. Wireshark.