Cell Phone Forensics

Lars Wolleschensky

17.08.2007

Seminararbeit
Ruhr-Universität Bochum

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

Contents

1 Introduction

Introduction
Mobile Phones play an important part in life today. In 2006 nearly 80% of all private homes in Germany owned a mobile phone, that are roughly 48,7 million mobile phones. The market is divided between Nokia (34,8%), Motorola (21,1%), Samsung (11,8%), Sony Ericsson (7,4%), and LG Electronics (6,3%) (Source Gartner: `www.gartner.com`).
So it is comes as no surprise that mobile phones are found with an increasing frequency at crime scenes. Mobile phones can play a cardinal part in a persons life, not only as a means of communication but also as an organizer or a camera. So there is a high chance of finding useful information about the owner of a phone. In connection with a possible crime a phone can hold various clues starting from contacts over call history to SMS messages. Police forces start to discover the usefulness of mobile phones in an investigation. At the moment the field of mobile forensics isn't fully developed. In some countries like the USA it isn't even recognized as a forensic science. Nevertheless the field is quickly expanding. This paper tries to give an outline of current practices and a future outlook.

2 The Forensic Process

There are many different guidelines for the forensic process. This is a brief summary of NIST ”Guidelines on Cell Phone Forensics” [WJ07]
.
Preservation and Documentation

In gathering the evidence it is important not to disturb the crime scene. One can not simply remove the mobile phone from the crime scene. Care has to be taken to preserve other forms of evidence like finger prints and DNA traces as well. Furthermore as with every piece of evidence proper documentation is need. This documentation should include at least some pictures with the undisturbed/unmoved phone as well as information about the time and location of the accusation. It is also important to note whether the phone was switched on or not.

Acquisition

In this phase actual data is gathered from the device. This gathering can take various forms. In an ideal case the data is forensically copied from the phone as well as from the SIM Card. In some cases technical difficulties can prevent a digital accusation of the device. In a worst case scenario only screen captures of the phone can be gathered.

Examination and Analyses

Now the gathered data is anlyzed for clues regarding the possible crime. These clues can take various forms for a closer analysis see below. The examination can either be done by hand or with the help of software tools. There are different software tools available for that purpose. It is important to use different software tools. There is no silver bullet and so care has to be taken not to miss a crucial piece of evidence solely because one particular tool didn’t have the right feature.

Reporting

The last step is the most important. Between the gathering of evidence and the presentation in court a significant amount of time can pass. An examiner must be able to present his evidence in a conclusive manner and offer the other party information about the tools and methods used. The evidence is useless if its not admitted in court and that can happen if the authenticity of the evidence is questioned because its origin or its acquisition isn't documented properly.

3 Types of Evidence

Address book:

The address book stores different contact information. With the help of the address book it is possible to gain an insight in the social network of the suspect. It can be used for example to link a suspect to a victim.

Call history:

The call history offers a deeper insight into the activities of the owner before the acquisition of the mobile phone occurs. One can see the last in and out going calls as well as their duration. This information can be used to draw indirect conclusions as well.

Short Message Service (in new phones emails as well)

The SMS messages as well as email offer concrete information in contrast to the call history and the address book which only offer indirect information. They can contain actual words written by the owner or intended for the owner which can serve as evidence in court.

Calender

The calender gives an overview over past and planned activities of the owner. It can be used to link the owner to certain location and times as well as indicate possible witness.

Other Media

Newer mobile phones can contain a host of other information as well.

First there is the camera. Pictures or movies can contain evidence as well. Not only in thier content but also in the form of the Exchangeable Image File Format, exif (data embedded in the file giving further information). It is possible that a perpetrator took a picture as a trophy of the crime. The exif data can be used to determine the exact date and time a picture was taken in some cases even the location. Some mobile phones are equipped with a GPS receiver. This receiver can store information about locations and times independently from applications running on the mobile phone. So the owner can be linked to possible crime scenes or alibis.

4 Current Problems

There are many problems facing mobile forensics. This paper will look at them in the order in which they are encountered during an examination.

The first problem occurs when the mobile phone is found on the crime scene. If the phone is switched off everything is fine but if the phone is switched on there is a problem. If the phone is left on it is possible to tamper with the evidence. Certain models can only store a specific amount of data, for example, only 20 SMS. If the criminal wants to destroy the evidence he simply sends 20 meaningless messages from another phone and all the evidence is lost. Similar scenarios are possible for incoming calls, but the biggest threat is remote wipe. Some business solutions in more complex phones offer a remote wipe option. This feature is indented for business customers who lose there phone and don't want to disclose company secrets. A criminal could use the feature to send the remote wipe command to a phone found on a crime scene to delete all data from it. On the other hand switching the phone off has certain drawbacks as well. If the phone is PIN locked the investigator has to contact the phones wireless provider in order to unlock it to gain excess to the information stored on the SIM card. In practice this isn't a major problem but switching the phone off causes the loss of all data stored in RAM. In some phones also data on SIM cards like the location register is deleted automatically. Again evidence is lost.
The third option is to leave the phone on but remove it from the network. This can be done by using Faraday bags which in theory prevent any radiation leaking from the network to the phone. This is only theory because if the phone is left on and isn't on the network it starts searching for the network through heightening its antenna output. This increases the energy consumption and reduces the battery lifetime. So somehow the phone has to be connected to the electricity grid. The cable connection reduces the effectiveness of the Faraday bag.
Different countries have solved these problems in various ways. The best practise guide in the United States recommends using Faraday bags where instead in the United Kingdom and Holland it is recommend to switch the phone off.
In new models there is a solution built in. The flight modus disconnects the mobile phone from the network if the customer wants to use the other features of the phone while flying. But in order to utilize this feature the investigator must know whether a particular phone has the feature or not directly at the crime scene which requires him to stay up to date with all the current models which isn't an easy task.

The next problem is to identify the phone. There are many different manufactures which all offer a host of different models with new models becoming available almost monthly. If a phone is found on a crime scene it has to be identified before the investigation can begin in order for the specialist to familiarize himself with it. There are different ways of doing this. Usually the logo of the manufacturer and the wireless provider are displayed on the side. But this is only a starting point. There are some web sites which try to help. Most notability `www.gsmarena.com` and `www.phonescoop.com`. Both pages have a huge list of phones with pictures and links to the manufacture. After a little research the investigator can usually identify the phone he has found.

Now the problem of connectivity and power arises. As mentioned above if the phone is left on it has to be charged during an investigation, since the battery of most phones won't last much longer then a week. Again there are many models by many manufacturers all requiring different power connectors. The only feasible option for the investigator is to have most of the cables at hand or after the phone is identified go to the proper store and buy the right power cable. This scenario must also be considered if the investigator chooses to switch the phone off on the crime scene, since it has to be powered up for the investigation. After the phone is switched on it automatically tries to reestablish a connection with the provider network. This isn't that big a problem anymore because the phone can be handled in a very controlled situation and most forensic labs have areas which are protected by a Faraday cage from the outside interference.

The bigger problem is to connect the phone to a PC in order to investigate it forensically. The older the phone the bigger the problem is. Again there is no standard for an interface and each manufacture has developed its own bus and interface and these systems have developed over time as well. This leads to a host of different cables. Today its slightly easier because most phones offer a USB connection for the customer to upload ring tones or other media. The same connection can be used for the investigation. But some manufactures (e.g. Motorola) change the PIN definitions in order to force the customer to use their cable.

The investigator has various options to overcome this problem. There are many different software solutions to help investigating a mobile phone forensically. Usually the software is bundled with cable kits for establishing the connection. This is very helpful for commonly used phones. For rare models connection cables have to be bought individually. But one has to be able to analyze new models as well. Some software manufactures (Susteen, Parabeen) offer deals that provide cables for newer models for a time up to two years after purchasing their software.

The next problem is to chose the right software for a particular phone. As

mentioned above there are many different software or hardware solutions available. Each of them has certain advantages or disadvantages both with regards to models supported and software features. Here the investigator has to fall back to previous experience. In an ideal world he would have seen the phone model before and know which software works best. In the real world the investigator faces new phones as well. Here he has to be very careful not to destroy evidence. There are various recommendations how to proceed.
First of all the investigator should download the manual of the phone from the manufacture to familiarize himself with the features and capabilities of the phone. It also helps to read various forums in the internet which try to offer help the to investigator.

After the initial research it is recommended to buy a phone of the same model to test the functionality of the software. Furthermore it is paramount not to relay on a single software solution. While testifying in court it's important that one can show that the same results were obtained while using different methods and so giving further credibility to them.

Giving credibility to results is not as easy as it seems. All mobile phones have an internal clock which changes data in the memory as well as wear leveling. Wear leveling is a process that tries to maximize the life time of the flash memory in a mobile phone. Flash memory can only be written and erased a certain amount of times. Wear leveling uses software and hardware to ensure that all parts of the memory are used systematically and thus the overall lifetime is as long as possible. Both processes make using checksums meaningless. In hardisk forensics checksums are used in court to prove that the evidence hasn't been tampered with and to show that the image from which the evidence is optioned is forensically the same as the original.
Since this is impossible repeatability is a big issue. Repeatability ensures that the same results are optioned if the same methods are used. Since checksums don't work it is important to document the forensic examination so that the opposing party can verify the results. If the same results are found using different software tools and methods the position of the examiner is strengthened considerably.

Last but not least there is the SIM card in the mobile phone. Data can be stored independently, from the mobile phone, on the SIM card. An interesting fact is that the SIM card offers features like last dialed numbers (most SIM card can store up to five) but the manufactures usually implement the feature on the phone. This can cause redundancy and can be helpful in investigations. The SIM card started out with relatively small storage space. Today SIM cards with up to 4 Megabytes are commercially available.
The SIM card holds important information like the Location Information File (LOCI). In the LOCI the investigator can find information about the last cells

in which the phone was active. The information is retained after the phone is powered down but the file can contain more than one cell and it is up to the investigator to establish the last movements of the phone from that file. For a detailed discussion see [AS07]
Another problem is the SIM lock. SIM's and data on there can be secured using a PIN (Personal Identification Number). One has only three tries at the SIM and then 10 tries for the PUK (Personal Unblocking Code). If a phone is found it is best practice to ask the owner for the PIN otherwise the only solution is to phone the manufacture and ask for the PUK. In order to option the PUK one must know the ICCI (Integrated Circuit Card Identifier). This number is usually found printed on the surface of the SIM.

5 Current Developments

Looking into the future of mobile forensics there are many developments on the horizon. As always some are good and others seem to throw up obstacles.

Naturally there is Moors law. Mobile phones will continue to get more powerful in processing power as well as in storage capacity. On the one side this will open up possibilities for new applications and on the other side there is more storage space to be analyzed. In theory this shouldn't cause any major problems because the same law applies to the hard and software the examiner uses and so he should be able to cope with it.
But there are bigger problems. Some mobile phone manufacturers are planning to encrypt their mobile phones as well as the data stored on them. For them this step is naturally because the operating system on the phones is their intellectual property. They have spent money to develop it and want to make money with it. Furthermore it can serve as the basis for future gains. With Digital Right Management (DRM) and phones becoming more popular there is an increasing market for other applications developing and so the companies are trying to protect their marked share.
This can cause problems for the investigator. Almost all current tools will not work with a strong encryption system in place. Furthermore, even if data like a SMS is recovered it will be in its encrypted form and so without the proper key almost useless. The investigator would have to depend on the cooperation of the software manufacture in almost all investigations which could lead to a lot of hussel and overhead.

But there are positive developments as well. Current tools are starting to depend on an interface of the Joint Test Action Group (JTAG). JTAG is/was original designed to test circuit boards in particular processors, memory chips and physical connections.
The interesting thing about it is that it could provide direct access to the processors and memory banks without rellying on the operating systems. On the downside in order for this to work one would either need to know the exact instruction set of the processor or the memory banks involved. In practice this is only known to the manufacture of the chips and the software.
But there are already some tools out there which make use of JTAG. These tools are called Flasher Boxes. Models include Smart-Clip (Motorola), N-Box (Nokia) and Tornado Box. The problem is that with very few exceptions these tools were

developed by the Black hat community to flash phones, break pin locks and alter operating systems. Nevertheless there are some current papers [MBR07] and [Har04] that try to utilize them for mobile forensic purposes. At the moment it is possible to read the memory banks of a few models. The only problem is that it is in fact a raw hex dump. The data is fragmented and includes useful bits as well as the operating system. In some cases like the Nokia series 30 and 40 it has been possible to reserve engineer the file system allowing the investigator perfect access to all the data stored on the phone. On the other side if nothing is known the data looks like random numbers.

It's up to the investigator to figure out the usefulness of information. At the moment this process works in practice but is not approved in court. Nothing is officially known about the Flasher Boxes and there workings because they were developed in the black hat community and the reverse engineering is also done by people which have nothing to do with the companies which developed the file systems. So it can not provide a solid base for a case. But as mentioned before products which have official approval are in development.

6 Conclusions

As one can see the field of mobile forensics offers many possibilities for the investigator but there are still many hurdles to overcome before its full potential can be reached. With an ever changing mobile phones market this area will always have new challenges for an investigator. But its usefulness in helping to solve a case can't be underestimated.

Bibliography

[AS07] Paolo Gubian Antonio Savoldi. Sim and usim filesystem: a forensics perspective. *Proceedings of the 2007 ACM symposium on Applied computing*, 2007.

[Har04] Michael Harrington. *Hex Dumping Primer*. 2004.

[MBR07] Coert klaver Ronal van der Knijff Marcel Breeuwsma, martien de Jongh and Mark Roeloffs. Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal*, 1, 2007.

[WJ07] Rick Ayers Wayne Jansen. *Guidelines on Cell Phone Forensics*. 2007.