Digital Forensics on Small Scale Digital Devices

Christian Bäcker

23.07.2009

Seminar Topic: Covert Channels and Embedded Forensics
Advisor: Daehyun Strobel

Seminararbeit
Ruhr-Universität Bochum

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

Contents

1 Introduction

Small Scale Digital Devices (SSDD) can be seen as a subgroup of embedded systems. An embedded system is in general a small computer with a special purpose to perform one or a few dedicated functions, e.g., a controller. The system basically consists of a microprocessor, a non-volatile memory (mostly flash) and a volatile memory (RAM) and connectors and is usually embedded as part of a complete device. Additional parts can be added to the system by design or as required. Because the embedded system is adapted to its purpose, its size and costs can be reduced. An SSDD is such a device with several appropriate build-in attachments, e.g., a graphic or network controller. Harrill and Mislan covered the terminology SSDD in [HM07] and grouped them into five categories:

- Embedded Chip Devices,
- Personal Digital Assistants (PDAs),
- Cell Phones,
- Audio / Video Devices, and
- Gaming Devices.

With the size shrinking of transistors and other device parts either more and more functionalities can be integrated into a predefined chip size or the device can be built smaller. As a consequence, many devices cannot be assigned to only one category, e.g., multimedia smart phones with built-in digital cameras.

Such systems find their way into our normal life, e.g., in form of cell phones, MP3 player, personal organizer, router, game consoles or modern network-capable TVs. SSDDs can be used to save several personal information like contacts, photos, calendar and notes. They started to displace classic paper helpers like schedules and address books. Therefore it can be supposed that SSDDs play an important role in forensics. An SSDD can also be a non-active device, like a USB (flash) drive, which must be considered in digital forensic analysis.

The statistics of the Federal Statistical Office of Germany from January 2007 [oG07] show that the distribution of SSDDs exceeds the distribution of PCs, see Table 1.1. That is why the necessity of forensic analysis of SSDDs increased in the last few years. Forensics on SSDDs is a very young field of science and although there is a great progress in developing analyzing tools and research, this field lags behind other forensic fields. Concurrently Anti-Forensics, the science of preventing forensic analysis, is more difficult because of the small size of the devices and the user's restricted data accessibility [vdK07].

At the moment cell phones have the greatest distribution of all SSDDs. So it is no surprise that there exist a lot of public information on cell phone forensics.

	Equipment Rate[1] per 100 Households in Percent	Equipment Stock [2] per 100 Households as Counts
MP3 Player	29	41,4
Camcorder	20	21,9
Digital Camera	48,7	59,4
PC	72,8	110,9
Cell Phones	81,8	141,4

Table 1.1: Federal Statistical Office of Germany 01/01/2007 GENESIS-Online [oG07]

But because of the similarity of the basic architecture, most realizations in cell phone forensics are also applicable onto other SSDDs. The CPU to memory bus architecture of SSDDs is similar to the PC except the used memory type and the additional secondary storage interface [Wil06]. Differences between SSDDs mainly exist in manufacturer hardware, e.g., cable connectors, and software, e.g., graphical user and application programming interfaces.

This paper is organized as follows: Section 2 gives a brief overview of the forensic process in general. After this, we will describe how the content of the storage memory of SSDDs can be recovered, resulting in a memory image. At last there will be some short hints in Section 4 how the data can be obtained from the memory image and which data are expected.

There are papers, websites and books like [Ges06] which describe how data can be extracted out of a memory image in detail but only a few how a memory image is generated from an SSDD. Hence, we focus on the generation of the memory image in this paper. We assume that the device was forensically taken from the crime scene, so that we must not care to destroy biometric data, e.g., fingerprints, or other evidence, e.g., place of device on crime scene.

[1] The equipment rate is the statistical measure of how many households have a specific good. For example, a 73% equipment rate of cell phones means that 73 out of 100 households have at least one cell phone. The equipment rate is calculated by the number of households in which there is a relevant durable consumer good, put in relation to the expanded number of households × 100.

[2] The equipment stock is the statistical measure of how many goods there are in 100 households. For example, an equipment stock of 114 cell phones per 100 households means that some households have more than one cell phone. In the case of multiple equipment, the equipment stock is higher than the equipment rate. The equipment stock is calculated by the number of relevant durable consumer goods in the households, put in relation to the number of extrapolated households × 100.

2 The Forensic Process

In short an analysis has to answer the questions when, where, and how a specific crime occurred. As stated in [FV05] the question of the “trustworthiness of information” must be answered evidentially in a forensic analysis. To achieve this and to stay in touch with actual developments, one has to regularly exercise the forensic process on example devices.

Although the procedures of the forensic analysis vary in dependency of the institution, three principles are common. We present them here as laws because of their importance. The first law of forensics is to *document all and everything.* You cannot have too much documentation and only with a good documentation one can follow the process evidentially. The second law is to *avoid changes and contaminations.* This is obvious but sometimes difficult, e.g., if you want to save the contents of a volatile memory. One attack that can be applied on PCs is the cold boot attack [HSH$^+$08]. It exploits the effect that the data loss of a non-powered RAM can be retarded by cooling the memory down. E.g., by connecting an alternative boot device the content of the memory can be read out. However, while this is a very effective attack on a PC, on SSDDs we can neither dismount the RAM - usually it is soldered on the printed circuit board - nor connect an alternative boot device for memory imaging. Also, wear leveling or state changes cannot always prevented. Wear leveling is a dynamic process to maximize the life of a flash memory by rearranging pages and/or blocks continuously. The purpose is that the memory is used evenly. As the most wear leveling algorithms are kept secret by the manufacturer data changes are unpredictable [BdJK$^+$07]. The third law states that *only competent people who can explain their actions must have access to the original device.* With respect to the required level of evidence the degree of training and expertise can vary, e.g., when an analysis is made for a private person and not a court.

The NIST[1] guide lists principles which suggests that the person with the overall responsibility should ensure the compliance with the governing laws.

The NIST also suggests to create different roles for the investigation, where one person can perform more than one role [AJ04]. A strict differentiation of the roles and their responsibilities is useful. The roles are first responders, investigators, technicians, forensic examiners, and forensic analysts. These people build an incident response team and should train together, such that in an incident the damage, attack methods, and possible results and consequences for the

[1] National Institute of Standards and Technology

organization can be evaluated in a very short time.

The investigation itself is divided into the five following steps:

Preparation of Investigation

An authorization of investigation is needed from the management, especially for external or non-police employees. Otherwise the investigation could be a reason for another investigation. This should prevent that an employee tampers with evidence or that privacy is broken by viewing sensitive data from unauthorized people. Also the assignment and goal of the investigation is to be set.

Preservation of Evidence

This step is concerned with the behavior at the crime scene, where all evidence is collected. The evidence must not be modified such it can be used at court. This involves the security of the own investigation area and used tools, too.

Imaging

Depending on the situation, *imaging* means getting information from a running system or making a bit-to-bit memory copy for later analysis. The copy should be made as fast as possible after the incident.

Analysis and Rating of Gained Information

This step has no time critical dependencies because the data is permanently saved in an image. At this step the image is examined for any sort of data. Then the data is reconstructed and sorted into categories, e.g., multimedia, text, deleted data etc. If possible, when the forensic specialist was given criteria, the data is not only analyzed but also relevance weighted.

Documentation

As already mentioned, an extensive documentation is indispensable for a forensic analysis. It is important to document instantly all doings and used hardware and software through the analysis. Experiences showed that information and activities that are not recorded instantly are never documented [Ges06]. At the end of the documentation the findings are summarized and explanations to the conclusions are given.

3 Data Acquisition

One must be prepared before trying to examine data of a device. Therefore it is best practice to have an identical device for tests and deep (and sometimes destructive) investigation. For a deep inspection all unknown built-in chips have to be identified by noting the written part number and search for the device and chip datasheet. This is important because a new chip with new (unknown to the analyzer) features could be built-in. Investigating available firmware updates can also give useful hints. After an example investigation one has to check if all expectations were achieved.

The question "Leave it on or switch the device off?" is tricky for SSDDs. On the one hand the volatile memory must be saved.On the other hand there can be a memory manager with a wear leveling algorithm, which can overwrite deleted data such that this data is unrecoverable. For SSDDs volatile memory is usually only used as CPU memory to work as cache and to hold state information. Therefore, it should be saved to get information about possible temporary data or connected networks. After this the SSDD should be switched off by removing the battery. The memory manager must not be able to overwrite data because overwritten data is not recoverable. Leaving the SSDD on, connecting it to a recharger and putting it into a faraday cage is not a good practice because the memory manager continues his work. The SSDD would recognize the network disconnection and therefore it would change its status information that can trigger the memory manager to write data [Wil06]. The non-volatile memory saves all other data, e.g., user information and application data. Nowadays mostly flash memory is used in SSDDs as internal non-volatile memory. Additionally, this memory can often be extended, which is discussed in the following.

3.1 External Memory

External memories are, e.g., SIM (subscriber identity module), SD (secure digital), MMC (multimedia card) and CF (compact flash) cards. For external memory and the USB flash drive an appropriate software, e.g., the Unix command "dd" is needed to make the bit-level copy. Furthermore USB flash drives with memory protection does not need special hardware and can be connected to any computer. Many USB drives and memory cards have a write-lock switch that can be used to prevent data changes, while making a copy. Otherwise, if the USB drive has no protection switch a write blocker [Wik09] can be used to mount the drive in a read-only mode or, in an exceptional case, the memory chip can be desoldered. The SIM and memory cards need a card reader to make the copy. The SIM card is soundly analyzed, such that it is possible to recover (deleted) data like contacts or text messages [Wil06].

3.2 Internal Memory Recovery Methods

This section describes various possibilities to save the internal storage, nowadays mostly flash memory.

3.2.1 System Commands

SSDDs do not provide the possibility to run or boot from CD, connecting a network share or another device with clean tools. Therefore the systems commands could be the only way to save the volatile memory of an SSDD. With the risk of modified system commands it must be estimated if the volatile memory is really important. A similar problem arises when no network connection is available and no secondary memory can be connected to an SSDD because the volatile memory image must be saved on the internal non-volatile memory, where the user data is stored and most likely deleted important data will be lost.

System commands are the cheapest method, but imply some risks of data loss. Every command usage with options and output must be documented.

3.2.2 Device Interfaces

For cell phones and PDAs exist complete solutions to extract data from the device through the hardware interface.

User Interface

The user interface can be utilized to investigate the content of the memory. Therefore the device is used as normal and pictures are taken from the screen. This method has the advantage that the operating system makes the transformation of raw data into human interpretable information. In practice this method is applied to cell phones, e.g., “Project-a-Phone”, PDAs and navigation systems [Cas03]. The disadvantage is that only data visible to the operating system can be recovered and that all data are only available in form of pictures.

AT Commands

AT commands are old modem commands and can therefore only be used on a device that has modem support. Using these commands one can only obtain information through the operating system, such that no deleted data can be extracted [Wil06].

Flasher Tools

A flasher tool is a manufacturer depending programming hardware and/or software that can be used to program (flash) the device memory, e.g., EEPROM or flash memory. These tools mainly originate from the manufacturer or service centers for debugging, repair, or upgrade services. They can overwrite the non-volatile memory and some, depending on the manufacturer or device, can also read the memory to make a copy, originally intended as a backup. The memory can be protected from reading, e.g., by software command or destruction of fuses in the read circuit [SD95]. Note, this would not prevent writing or using the memory internally by the CPU. The flasher tools are easy to connect and use, but some can change the data and have other dangerous options or do not make a complete copy [BdJK+07].

JTAG

Existing standardized interfaces for reading data are built into several SSDDs, e.g., to get position data from GPS equipment (NMEA) or to get deceleration information from airbag units [Cas03].

Not all SSDDs provide such a standardized interface nor exist a standard interface for all SSDDs, but all manufacturer have one problem in common. The miniaturizing of device parts opens the question how to test automatically the functionality and quality of the soldered integrated components. For this problem an industry group, the Joint Test Action Group (JTAG), developed a test technology called “boundary-scan”. This technique adds a shift register to each integrated component. The shift register is disconnected at normal device usage, such that it does not consume any power or influence the device. The register is used to probe and set the pins of the device component and makes it possible to read the memory. A test access port makes the shift register direct accessible. Alternative the CPU supports the boundary-scan, then the components are tested through the CPU controlled bus system.

For interoperability between components from different manufacturers the JTAG has standardized the procedure for implementing the boundary-scan in IEEE 1149.1. Therefore this technique is frequently called the JTAG-standard.

Despite the standardization there are four tasks before the JTAG device interface can be used to recover the memory. To find the correct bits in the boundary-scan register one must know which processor and memory circuits are used and how they are connected to the system bus. When not accessible from outside one must find the test points for the JTAG interface on the printed circuit board and determine which test point is used for which signal. The JTAG port is not always soldered with connectors, such that it is sometimes necessary to open the device and resolder the access port [BdJK^{+}07]. The protocol for reading the memory must be known and finally the correct voltage must be determined to prevent damage to the circuit [Wil06].

The boundary-scan produces a complete forensic image of the volatile and non-volatile memory. The risk of data change is minimized and the memory chip must not be desoldered. Generating the image can be slow and not all SSDDs are JTAG enabled. Also it can be difficult to find the test access port [vdK07].

3.2.3 Forensic Desoldering

The last and most intrusive method to get a memory image is to desolder the non-volatile memory chip and connect it to a memory reader. This method contains some potential danger of total data destruction. It is possible to destroy the chip and the content because of the needed heat at desoldering. Before the invention of the BGA[1] technology it was possible to attach probes to the pins of the memory chip and to recover the memory through these probes. The BGA technique bonds the chips directly onto the PCB[2] through molten solder balls, such that it is no longer possible to attach probes.

Desoldering the chips must be done carefully and slowly, such that the heat does not destroy the chip or data. Before the chip is desoldered the PCB is baked in an oven to eliminate remained water. This prevents the so-called popcorn effect, at which the remained water would blow the chip package at desoldering.

There are mainly three methods to melt the solder: hot gas, infrared light, and steam-phasing. The infrared light technology works with a focused infrared light beam onto a specific IC and is used for small chips. The hot gas and steam cannot focus as much as the infrared technique.

After desoldering the chip a re-balling process cleans the chip and adds new tin balls to the chip. Re-balling can be done in two different ways. The first is to use a stencil. The stencil is chip dependent and must fit exactly. Then the tin-solder is put on the stencil. After cooling the tin the stencil is removed and if necessary a second cleaning step is done. The second method is the laser re-balling. Here the stencil is programmed into the re-balling unit. A tube/needle is automatically loaded with one tin ball from a supply tank. The ball is then heated by a laser, such that the tin-solder ball becomes fluid and flows onto the cleaned chip. Instantly after melting the ball the laser turns off and a new ball falls into the tube/needle. While reloading the tube/needle the re-balling unit changes the position to the next pin.

A third method makes the entire re-balling process unnecessary. The chip is connected to a adapter with Y-shaped springs or spring-loaded pogo-pins. The Y-

[1] Ball Grid Array

[2] Printed Circuit Board

shaped springs need to have a ball onto the pin to establish an electric connection, but the pogo-pins can be used directly on the pads on the chip without the balls [BdJK^{+}07] [Wil06].

The advantage of forensic desoldering is that the device does not need to be functional and that a copy without any changes to the original data can be made. The disadvantage is that this process is very costly. The re-balling devices are expensive and there are some risks of total data loss. Hence, forensic desoldering should only be done by experienced laboratories [vdK07].

4 Data Examination

We are not giving a manual on how to extract the data out of the memory image. A desired goal is to work on a full bit-level copy of the memory because it is an unmodified memory image. Software tools can interpret and extract the data, even if the data was deleted by the operating system. The memory copy has also the advantage that it can be copied and analyzed by more than one tool or analyzer at once. As an increasing number of embedded systems uses high level file systems, similar to the file systems of PCs, methods and tools can be taken over from hard disk forensics or only needs slightly changes [BdJK$^+$07]. Mostly used on NAND memory is the FAT file system [vdK07]. A difference is the used block size, which is larger than 512 byte for hard disks and depends on the used memory type, e.g., NOR type 64, 128, 256 and NAND 16, 128, 256, or 512 kbyte.

Different software tools can extract the data from the memory image. One could use specialized and automated forensic software products or generic file viewer like any hex viewer to search for characteristics of file headers. The advantage of the hex viewer is the deeper insight into the memory management. But working with a hex viewer means a lot of handwork and file system as well as file header knowledge. In contrast, specialized forensic software simplifies the search and extracts the data but may not find everything. AccessData, The Sleuthkit, EnCase, only to mention some, are forensic software products to analyze memory images [AJCD05]. Since there is no tool that extracts all possible information, it is advisable to use two or more tools for examination. Also it is maybe a good strategy not to search for any special data because one may find them, but misses all other interesting stuff. A better strategy searches for any data and then evaluate the findings.

4.1 Which data exist?

While the data of some SSDDs like routers are limited, the data that can be found on a cell phone constantly increases. At the earlier days of cell phones only telephone numbers were found. Today additional information like calendar, GPS positions, messages, notes, pictures, or movies are normal on cell phones.

Interesting data that can be found on SSDDs are, e.g.,

- (multimedia) files (sounds, music, images, video, podcasts)
- messages (SMS, MMS, Twitter, Chat)
- eMails

- browser history/bookmarks/cookies
- personal information (Calendar, Contacts, Notes)
- log files (call, network, application)
- maps (Google, OpenStreetMap)
- connection information (Bluetooth, WLAN, VPN)
- GPS positions
- running processes
- routing tables
- network and connectivity statistics
- boot sequence, default libraries
- . . .

As mentioned earlier SSDDs can get more functions, e.g., to act as a storage device, and a steady development of new applications can create new data. Hence, the data list must be updated as necessary and can never be viewed as complete. Especially because of the storage functionality of many devices, any kind of file type could be found during the examination

5 Conclusions

In this paper, we gave an overview of SSDDs and how they are related to embedded systems. After a short description of the forensic process, we discussed several techniques to recover the volatile and non-volatile memory. At last we gave a small list of interesting data that can be found on SSDDs and how the memory image can be analyzed.

Because of their great spreading, cell phones, MP3 players, and PDAs are well analyzed by now.

It can be observed that more and more devices getting networking capabilities, e.g., TVs, game consoles, refrigerators, Blu-ray player. Although some of the mentioned do not fall under the term SSDD they use the same techniques. Therefore the here discussed methods are applicable to them, too. With this in mind, it can be assumed that the probability raises that an unusual device is needed for evidence and has to be analyzed one day. Therefore it is important to develop generic forensic methods, procedures and memory interfaces for SSDDs. The JTAG interface is standardized and seems useful for manufacturer for their quality assurance on integrated circuits. For the forensic process the JTAG interface is interesting because it can help generating a memory image from the non-volatile and volatile memory without changing data and without much effort.

A problem is the replaceability of memory cards, e.g., in digital cameras or in cell phones with build-in digital camera. It must be proved that a picture, which was found on the memory card, was really made by the digital camera. For such problems other techniques like (lens) noise analysis is needed [KMM+06].

Still a big problem for forensic analysis is the deficit on detailed device documentation [MR05] [Wil06].

Bibliography

[AJ04] Rick Ayers and Wayne Jansen. *Guidelines on PDA Forensics.* National Institute of Standards and Technology, November 2004. `http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf`.

[AJCD05] Rick Ayers, Wayne Jansen, Nicolas Cilleros, and Ronan Daniellou. *Cell Phone Forensic Tools: An Overview and Analysis.* National Institute of Standards and Technology, October 2005. `http://csrc.nist.gov/publications/nistir/nistir-7250.pdf`.

[BdJK+07] Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff, and Mark Roeloffs. Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal*, Volume 1(Number 1), 2007. `http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf`.

[Cas03] Eoghan Casey. *Handbook of computer crime investigation - forensic tools and technology.* Academic Press, 2. edition, 2003.

[FV05] Dan Farmer and Wietse Venema. *Forensic Discovery.* Addison-Wesley Professional, 2005. Available at `http://www.porcupine.org/forensics/forensic-discovery/`.

[Ges06] Alexander Geschonneck. *Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären.* 2. Auflage. dpunkt.verlag, ix edition, 2006.

[HM07] David Christopher Harrill and Richard P. Mislan. A small scale digital device forensics ontology. *Small Scale Digital Device Forensics Journal*, Volume 1(Number 1), 2007. `http://www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf`.

[HSH+08] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Cal, Ariel J. Feldman, and Edward W. Felten. Least we remember: Cold boot attacks on encryption keys. In *In USENIX Security Symposium*, 2008. `http://citp.princeton.edu/memory/`.

[KMM$^+$06] Nitin Khanna, Aravind K. Mikkilineni, Anthony F. Martone, Gazi N. Ali, George T.-C. Chiu, Jan P. Allebach, and Edward J. Delp. A survey of forensic characterization methods for physical devices. *Digital Investigation*, 3:17 – 23, 2006. `http://dfrws.org/2006/proceedings/3-Khanna.pdf`.

[MR05] Christopher V. Marsico and Marcus K. Rogers. ipod forensics. *International Journal of Digital Evidence*, Volume 4(Number 2), 2005. `http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A8B3F3-94D2-F7E5-D32D97CF1539EBB4.pdf`.

[oG07] Federal Statistical Office of Germany. Ausstattungsgrad und ausstattungsbestand von haushalten (laufende wirtschaftsrechnungen): Deutschland, stichtag, gebrauchsgüter, 2007. `https://www-genesis.destatis.de/genesis/online/logon`.

[SD95] Tom Salt and Rodney Drake. Us patent 5469557 - code protection in microcontroller with eeprom fuses, 1995. `http://www.patentstorm.us/patents/5469557/description.html`.

[vdK07] Ronald van der Knijff. 10 good reasons why you should shift focus to small scale digital device forensics, 2007. `http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf`.

[Wik09] Forensic Wiki. Write blockers, 2009. `http://www.forensicswiki.org/wiki/Write_Blockers`, [Online; accessed 06-June-2009].

[Wil06] Svein Y. Willassen. Forensic analysis of mobile phone internal memory, 2006. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.6742&rep=rep1&type=pdf`.