Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

Android Forensics Techniques

Zlatko Jovanovic

Instructor Dr DeAndre Redd

International Academy of Design and Technology

January 28, 2012

Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

Abstract

Paper discusses different specific forensic techniques for examining Android mobile devices. Logical and physical acquisition techniques are defined and deeply described. Process for imaging device and data handling are described. Various commercial providers are examined. Strategies for circumventing the pass code and strategies for gaining root privileges are also described.

Keywords: Android device, electronic evidence, data extraction, logical techniques, physical techniques, NAND flash, JTAG, Chip-off, AFLogical, AFPhysical, adb pull.

Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

Contents

Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

Introduction to Android devices

Android devices came as a response to extreme success of Apple's iPhone on the handheld device market. Since the beginning in 2005, when Google bought the small company that developed Android operating system, Android Inc., and since its release in 2008, Android devices are constantly increasing their market share. According to Andy Rubin, the senior vice president of Google, there are over 700,000 Android devices activated daily (Wong, 2011).

The name of the device is based on the platform used in its built. Android was built on the Linux kernel 2.6 and is fully open source (Conti, 2008). Decision to release an open source is Google's strategy which was surprising for many. By doing that Google saves more than twenty percent drop in manufacturing cost just from the software savings (Wong, 2008).

According to Massé, manufacturers like Motorola, Samsung and Nokia, are moving toward Android Operating system (Massé, 2011). There is also an increasing usage of Android devices in enterprises. The capabilities of the handheld devices are so powerful that companies are implementing policies for their usage (Leung, 2011).

Android devices are made by various manufacturers, and its operating system and applications are developed by enthusiasts all over the World. The main characteristic of Android devices is its source code availability. This is a big down flow when it comes to the examination of the device by a computer forensic expert.

Fact that every manufacturer builds its own hardware for the Android device does not serve forensic examination of the device. With every new model on the market, forensic expert are dealing with new hardware and software solutions implemented in the new device. Each new model must be examined and researched first, in order to be able to adequately respond to the investigation requests. Theoretically, each new model of the Android family is a new electronic device which needs to be researched in order to formulate proper techniques needed for its examination.

Introduction to Android Forensics

Due to the huge number of different devices, Android forensics discipline is in expansion. Androids, and the other handheld devices, can hold vast information about the users and their habits. Forensic analysis of the handheld device can reveal some interesting information about the user that can help in an investigation. Usually users feel that the device is very personal, and that they are the only one who will ever have access to it. This is the reason that some very discrediting information could be found on handheld devices.

The concept of Android forensics consists of techniques to extract the most possible data from the device without losing, or altering the content of the device. Modification of the data or data preservation is the biggest problem when dealing with Android devices.

The technique that is most recommended is live acquisition due to the volatile nature of the device's memory. Live acquisition is recommended because the volatile memory can hold various data which could be of value for the investigation. The examples of data that could be found in the volatile, RAM memory are:

- Passwords
- Encryption keys
- Usernames

- Application data
- Data from system processes and services

There is a technique developed by security engineer Thomas Cannon which helps acquiring significant application data. The technique is using the Android's ability to dump the application memory to a file by sending the application a special signal - SIGUSR1 (Hoog, 2011). Tendencies are that there will be more solutions to help analysis of the Android memory in the future.

Android Forensics Challenges

Data in Android devices could be stored in several locations. It could be stored in either NAND flash, the SD card, or the network. Data that could be found in the Android devices could be broader than the data found in the personal computers. A reason for choosing the NAND Flash memory over the other types relies in its capabilities to store significant amount of data in relatively small physical size of the memory. Current technology went from 34 nm and 25 nm to 20 nm and can hold 128 GB of data. Micron, one of the makers of NAND memories states that "Our new 128Gb MLC NAND device provides the highest storage capacity of any single die on the market, enabling more storage for portable devices." (Micron, 2012). NAND flash memory is non-volatile and besides system files, it stores a significant portion of user's data. Examples of data found on the Android device are:

- Text messages (SMS/MMS)
- Contacts
- Call logs

- E-mail messages
- Instant messenger/ Chat
- GPS coordinates
- Photos/ Video
- Web history
- Search history
- Driving directions
- Social media clients (Facebook, Twitter)
- Calendar appointments
- Financial information
- Shopping history
- Music collection files and files sharing (Hoog, 2011).

Data found on the Android device while conducting live acquisition can hold information that is not possible to find in other form of acquisition. Therefore RAM memory can hold data such as:

- Passwords
- encryption keys
- usernames
- application data
- Data from the system processes and services (Hoog, 2011).

NAND flash was design with very small cell size for the low cost-per-bit of stored data. Technology behind this is an array of eight memory transistors connected in series (Jang-Gn, Jong Duk & Byung-Gook, 2009). The organization of the NAND flash memory is shown in Figure 1.

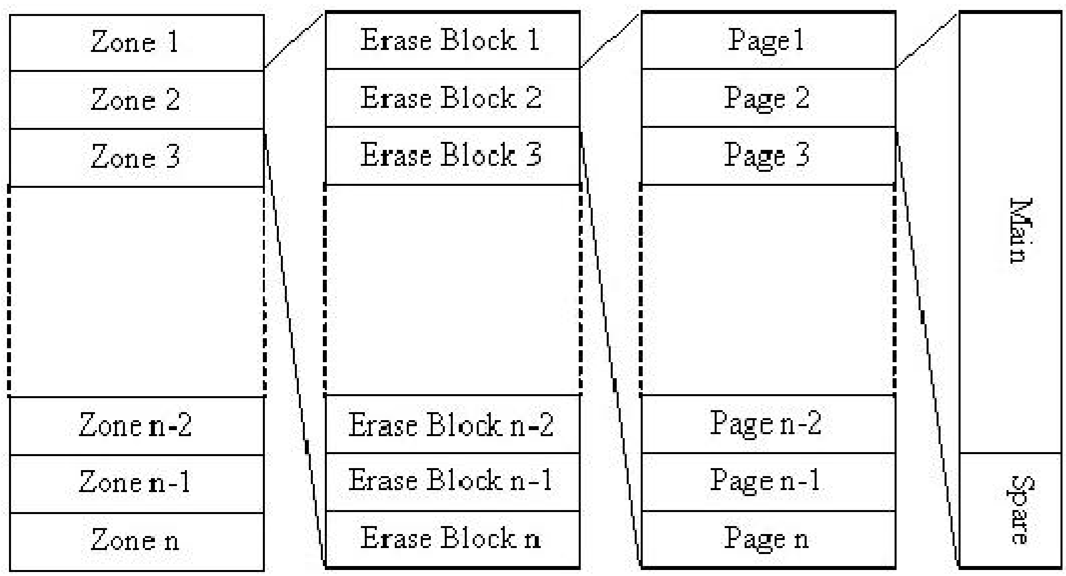

Figure 1. Dissection of NAND flash memory

Even though NAND flash memory has been on the market for a long time, looking from the technology development viewpoint, its design still represents a challenge for programmers and forensic analysts.

One of the challenges that will be bigger in the future is the virtual machine that could be found on the device (Edwards, 2011). This can cause various file systems found on the Android device beside the file system that originally appear on it. That would mean that Windows, Mac or other file systems could be found on the Android device.

Android vulnerabilities

Android vulnerabilities are still to be evaluated. The fact that Android devices are relatively new on the smart phones market, and constantly releases of new models and operating systems, influence experts not being able to determine all vulnerabilities and risks.

Android vulnerability is the main concern with corporations since there is no proof of the security, or not known precise risks. That is why the corporations' smart phones are widely targeted, and the exploitation of them is the main focus of the hackers.

Android Forensic Techniques

Procedures for handling an Android device

Procedures for handling the Android device are the same as the procedures for handling the personal computer or lap top. The procedures still have five steps that are very important to hold on to while handling the device. The five steps are:

- Identifying
- Preserving
- Acquiring
- Analyzing
- Reporting

As in the computer forensic investigation, the chain of custody must be followed as well. Regardless of whether the investigation is in the corporate environment or is a part of the criminal investigation, it is necessary to follow the rules for evidence handling. Any case in any time can end up in court. The best practice is that investigation should always be conducted as the case will be in the court of law. The important considerations while conducting the Android device investigation are:

- Chain of custody
- Detailed notes and final reports
- Validation of results by different tools or examiners
- Fact or opinion based testimony (Hoog, 2011).

Andrew Hoog thinks the four principles of electronic based computer evidence are of the essence. The four principles are:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

2. In circumstances where a person finds it necessary to access original data held on a computer or on the storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that law and these principles are adhered to. (Hoog, 2011)

Handling the Android device is different than handling personal Computer in the investigation. The nature of the handheld device that loses some important data if powered off makes the distinction from personal computer handling. It is also very important to secure device from locking down, accessing network or losing power.

Nena Lim and Anna Khoo are pointing out the dilemma that arises with the Android devices. Should the device be left on, or should it be powered off (Nena & Anna, 2009). If possible, the best solution would be to leave it on, and to extract data while it is on.

Techniques for securing the device vary from pass code procedures, through powering, to network isolation. On most Android devices, pass code locking could be circumvented by:

1. Increasing the timeout to prevent or postpone the screen locking.
2. Enabling the USB debugging and “stay awake” settings (Hoog, 2011).

Network isolation of the Android device is very important for the investigation. There is a possibility that the remotely access programs are installed on the device, and a remote wipe could be initiated. Andrew Hoog gives the table with advantages and disadvantages of different techniques for device network isolation. Hoog’s table is presented in table 1.

Technique	Advantage	Disadvantage
Put the device in Airplane	The device continues	You are modifying the device

mode. This requires that you have full access to the Settings menu.	running and temporal data remains intact. Disables cellular data network as well as Wi-Fi.com.	setting further. Only works if you have full access to the device.
If the phone is a GSM phone, remove the SIM card.	Easy to remove, effective in disabling all cellular voice, SMS, and data transmission.	Does not disable Wi-Fi.com or other networks. Does not work on non-GSM phones including CDMA and iDEN phones.
Suspend account with wireless carrier.	Effective in disabling all cellular voice, SMS, and data transmission for any phone.	Process may take some time and require a court order. Does not disable Wi-Fi.com or other networks.
Place device in a shielded bag, box, tent, or room.	Faraday shields prevent various types of network transmissions and can be effective approach if you cannot utilize any of the previous options.	There is some debate about the effectiveness of portable Faraday shields, notably Faraday bags. Also, while the transmissions are blocked, the device attempts to contact the cellular network repeatedly thus draining the battery. Cords cannot be inserted into the enclosure as they will transmit the signals. A shielded room dedicated for mobile

		examinations is ideal. However, they are quite expensive to build and maintain.
Turn the device off.	Completely effective in preventing all network transmissions.	The device state is modified and temporal data is lost. Pass code on reboot could be enabled, thus restricting access to the device.

Table 1. techniques for device isolation

Whichever technique used, it needs to be logged, and fully described and rationale.

For Andrew Hoog, the best technique is the Airplane mode.

Imaging Android device

Imaging the Android device is based on the imaging of the SD (Secure Digital) card or an eMMC (Embedded Multi Media Card) (Hoog, 2011). Android devices are made with SD cards as a sort of storage device to enable users to easily move their data: songs, pictures, videos and other files to other devices and computers. The process to image the card consisted of simply removing the card and image it using the USB write blocker. There are few challenges when it comes to the imaging the cards. Some devices, and in the future more of them, have an eMMC storage which is emulated SD card in the flash memory. The issue with these types of cards is that they are not removable. Second challenge is an application that runs from the SD card. To capture the unencrypted .apk files, the SD card must remain in the device (Hoog, 2011). The most common issue is that in order to remove the SD card, the battery needs to be removed first.

There are two methods of acquiring the image to be a forensically sound image. First method is attaching the device by the UMS (USB Mass Storage) interface to the forensic workstation and using the appropriate tool. Second method of acquiring the image uses dd on the Android device. This method requires adb port forwarding (Hoog, 2011)

Logical data acquisition

Data acquisition techniques could be logical and physical. Logical technique is based on the extraction of data which is allocated. To achieve this, the file system must be accessed. By allocated data, Hoog assumes data that is not deleted and that is still accessible on the file system. Logical acquisitions techniques are:

- ADB Pull
- Backup analysis
- AFLogical

ADB Pull

The technique is relying on the adb pull command which copies parts of the file system to the forensic workstation for further analysis. It is a free utility found in the Android SDK. Most of the forensically relevant files are not accessible without the shell permissions, unless a root access is available on the device. Copying keeps the file structure intact. This technique is useful in the following scenarios:

- On non-rooted devices, adb pull can still access unencrypted apps, user data such as browser history, and system information found in readable directories.
- On rooted device nearly all directories can be "pulled"
- Sometimes when using a physical technique, file systems such as YAFFS2 cannot be mounted. In that case a logical copy can be obtained by using the adb pull (Hoog, 2011)

Backup analysis

Backup analysis technique relies on the examining the backup data found in the SD card, or in "the cloud". Popular backup applications can take a backup of the device by using the Content Provider, and even the entire "/data/data" files if the root access is enabled. The backup applications give the opportunity to examine the files on different machines, with different operating systems. The existence of backup applications, and more important, the location where the backup files are stored, is an important information for the examination.

AFLogical

AFLogical is a free application developed by viaForensics. Application uses Content Providers to extract data. During the installation of the applications, the user is prompted to choose if the application is going to share the information with other applications. Also, the application can gain access to the Content Providers, like:

- SMS/MMS
- Contacts
- Calendar
- Facebook

- Gmail, etc.

This is the framework for the AFLogical. But the USB debugging must be enabled on the device. The current version of AFLogical can extract data from 41 Content Provider (Hoog, 2011).

Commercial providers

Besides the free applications for logical extraction of data, a number of commercial vendors have the forensic software that supports Android devices. Some of them are:

- Cellebrite UFED
- Compelson MOBILedit!
- EnCase Neutrino
- Micro Systemation XRY
- Paraben Device Seizure
- viaForensics' viaExtract

Physical data acquisition

Techniques that acquire physical image of the device usually produce more useful data than the logical techniques. All the deleted data is accessible with the physical technique. Also the data that was no longer used by the device and the system, was accessible with this technique. Physical acquisition techniques are:

- Hardware- Based
    - JTAG
    - Chip-off
- Software- based

- AFPhysical

JTAG

JTAG is a technique that uses test access ports (TAPs) of the printed circuit boards (PCB) for wiring and testing. By using the connections the central processing unit (CPU) is accessed. Major issue with this technique is locating and determining the pins. This technique requires soldering skills and extensive knowledge, because mistakes are not permitted, or data is lost. This one and the following technique should be the last resort.

Chip-off

Chip-off is the most destructive technique of all. Once pulled out, the chip usually cannot be put back. The Chip-off technique consists of three steps:

1. Physical removal of the NAND flash chip
2. Repairing the balls on the bottom of the chip, since the removal damages the balls.
3. Inserting the chip into the special device programmed to read NAND flash for the specific device.

The cost of the equipment and the destructive nature of the technique turn away examiners from using it more often.

AFPhysical

Technique developed by viaForensics. As Hoog lists the process for AFPhysical is next:

1. Acquire root privileges on the target device.
2. Identify NAND flash partitions which need to be imaged.
3. Upload forensic binaries to the target device.

4. Acquire physical image of NAND flash partitions.
5. Remove forensic binaries if any were stored on nonvolatile storage (Hoog, 2011).

For this technique it is mandatory to have root privileges. Advantage of this technique is that it works even if the device is pass code locked. Physical acquisition strategies that can be used after the acquiring the root privileges are:

1. Full nanddump of all partitions, including data and OOB.
2. A dd image of partitions.
3. A logical acquisition of files using tar.
4. A logical acquisition of files using adb.

Conclusion

Android Forensics is a field which constantly changes. New devices are on the market daily. It is up to examiner's experience and intuition to adapt to the new device and to choose technique that will most fit the investigation. Physical acquisition techniques will produce more data, but they are more complex. Logical techniques are simpler but focus mainly on undeleted data accessible through the Content Provider. Finally, forensic examiner should try to produce the most data from the simplest technique applied first.

Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

References

Betts, B., & Proven, L. (2011). Software Reviews: Mac 'Lion', Group Video, Mobile Security 10, Cerberus. Engineering & Technology (17509637), 6(7), 96-97. doi:10.1049/et.2011.0718

Conti, J. (2008). The Androids are coming. Engineering & Technology (17509637), 3(9), 72-75. doi:10.1049/et:20080912

Edwards, C. C. (2011). Calling Dr. Jekyll. Engineering & Technology (17509637), 6(3), 56-59. doi:10.1049/et.2011.0310

Gold, S. S. (2011). Will Holey handsets get caught 'App napping'?. Engineering & Technology (17509637), 6(8), 78-81. doi:10.1049/et.2011.0811.

Hoog, A. (2011). *Android forensics, Investigation, Analysis and Mobile security for Google Android.* Waltham, MA: Syngress.

Jang-Gn, Y., Jong Duk, L., & Byung-Gook, P. (2009). Various Flash Memory Devices of Novel Design. IETE Technical Review, 26(4), 247-257. doi:10.4103/0256-4602.52994

Lahiri, A., Dewan, R. M., & Freimer, M. (2010). The Disruptive Effect of Open Platforms on Markets for Wireless Services. Journal Of Management Information Systems, 27(3), 81-110.

Leung, T. (2010). Mobility gains momentum in enterprise space. *Computerworld Hong Kong*, *27*(10), 35.

Massé, D. (2011). With 24 Percent Share of Smartphones, Android Will Outshine "Nokisoft". *Microwave Journal*, *54*(4), 49-50.

Zlatko Jovanovic
zjovanovic@bulleproof.com
http://www.bulleproof.com

NENA, L., & ANNE, K. (2009). Forensics of Computers and Handheld Devices Identical or Fraternal Twins?. *Communications Of The ACM*, *52*(6), 132-135.

The teardown: the Logitech Revue set-top box for Google TV. (2011). Engineering & Technology (17509637), 6(7), 94-95. doi:10.1049/et.2011.0717

Wong, George. "Over 700,000 Android Devices Activated Daily." *Ubergizmo*. 21 Dec. 2011. Web. 26 Jan. 2012. <http://www.ubergizmo.com/2011/12/over-700000-android-devices-activated-daily/>.

Wong, K. (2008). The new kid on the block. *Networkworld Asia*, *4*(6), 35.