A Framework for Designing Benchmarks of Investigating Digital Forensics Tools for Mobile Devices

Maynard Yates

Florida Agricultural and Mechanical University
Department of Computer and Information Sciences,
Tallahassee, FL 32307-5100

maynard1.yates@famu.edu

Hongmei Chi

Florida Agricultural and Mechanical University
Department of Computer and Information Sciences,
Tallahassee, FL 32307-5100

hchi@cis.famu.edu

ABSTRACT

With the continued growth of the mobile device market, the possibility of their use in criminal activity will only continue to increase. While the mobile device market provides a great variety of manufacturers and models causing a strong diversity, it becomes difficult for a professional investigator to choose the proper forensics tools for seizing internal data from mobile devices. Through this paper, we will give a comprehensive perspective of each popular digital forensic tool and initiate discussion towards benchmarking key features and considerations of forensic analysis techniques.

Categories and Subject Descriptors

K.4.1. [Computers and Society]: Public Policy Issues - *abuse and crime involving computers*; D.4.6 [Operating Systems]: *Security and Protection--Access controls*

General Terms

Management and Security, Legal Aspects, and Verification.

Keywords

Digital forensics, handheld devices, mobile devices, forensics tools, Paraben CSI stick, cell Seizure, XRY, benchmarking

1. INTRODUCTION

There are only few benchmarks or standards set for digital investigations involving traditional computers and general guidelines and accepted best practices for network forensics. However, there aren't any for mobile forensics because they are still relatively new and still considered emerging fields in research and industry. Computer forensics precedents are just now being converted to standards to try and accommodate criminal investigations. Traditional computer forensics can be traced back as far as 1993 when the US Supreme Court Case, *Daubert v. Merrill Dow Pharmaceuticals*, set a precedent regarding the admissibility of digital forensic evidence. Courts were given discretion whether to accept scientific evidence

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. 49th ACM Southeast Conference, March 24-26, 2011, Kennesaw, GA, USA.
Copyright 2011 ACM 978-1-4503-0686-7/11/03...\$10.00.

based on the following criteria [2]:

- The theory or technique utilized must have been tested and that test must be replicable
- The theory or technique must have been subject to peer review and publication
- The error rate associated with the technique must be known
- The theory or technique must enjoy general acceptance within the scientific community

Earlier investigations where digital evidence was involved were categorized with traditional forensic science were governed by the *Frye* principles, where evidence gathered using "generally accepted practices" were admissible in court. As recently as 2000, both *Frye* and *Daubert* principles were revised, updated, and released as the Federal Rules of Evidence (FRE). [2]

Although similar in nature and concept to its desktop counterpart, mobile devices operate drastically different. Even though there are only five mobile operating systems that dominate the mobile device market, there are a wide variety of device manufacturers creating many more variants. The variants make it improbable to create a common, reproducible set of data to test for benchmarking and standardizing digital forensic techniques. [4] In this paper, we attempt to address those issues with designed benchmarks for specific operating systems.

There are a few ways that can be discussed in creating benchmarks for mobile forensics, for example by forensic tool or by operating system and in some cases device model. This case study will use forensic tools and mobile device operating systems as benchmarks categories. The forensic tools will encompass benchmarks for mobile device type, mobile device model, and time it takes to perform an acquisition while the mobile device operating systems category will consist of benchmarks for device models and network carrier. While we have established the benchmark categories of forensic tools and operating systems, the benchmarks themselves will be created according to the data types received from the forensic acquisitions during experimentation.

This paper is organized as follows: section 2 will discuss the forensic analysis of mobile devices, while section 3 will discuss tools available for forensics of mobile devices. Section 4 will discuss related work; section 5 will discuss proposed work and this case study will be carried out, followed by conclusion in section 6.

2. Forensic Analysis

Unlike traditional computers, two of the most important factors in a forensic investigation are the state of the device at the time of acquisition and radio isolation. [8] Legally, you can establish the chain of custody and document the entire investigation; but in order to perform an acquisition an investigator must take into account the state of the device whether it is On/Off. Regardless of device, an investigator should be aware of these issues.

2.1 Mobile Device Analysis

There are issues to consider about each operating system as an investigator prepares to forensically analyze a mobile device. There are two types of cell phone networks: code division multiple access (CDMA) and time division multiple access (TDMA). CDMA uses a spread spectrum technology using a special coding scheme thereby allowing multiple digital signals on the same channel, making CDMA less costly to implement, more efficient, and more secure than other cell phone network technologies. CDMA devices operate on variants of the 2G network standards, CDMA 1X, CDMA1XEV-DO (evolution data optimized), or CDMA1X EV-DV (evolution data voice). They also possess the following characteristics:

- Electronic Serial Number (ESN): This number is found on the compliance plate located under the phone battery and can be displayed as ESN DEC, ESN HEX, ESN or D. The ESN is a unique 32 bit number assigned to each mobile phone on a network. You will note that the ESN in its decimal format contains only decimal numbers, distinguishing it from its ESN HEX equivalent which will contain both decimal and alpha characters.
- Mobile Equipment ID (MEID): This number is 56 bits long, replacing the originally used ESN, because of the limited availability of the 32 bit ESN numbers.
- May or may not use a Subscriber Identity Module (SIM)

TDMA, which is better known by its variants Global System for Mobile Communication (GSM) & Integrated Digital Enhanced Network (iDEN), uses an allotted radio channel divided into time slots that allows each time slot to handle one call. Devices that operate on a TDMA network require a SIM card, or just SIM, for the device to operate. GSM is the largest mobile phone network in the world operating on 5 different bandwidths on most continents. GSM devices were originally derived from 2G network standards, like CDMA, but now operate on these variants General Packet Radio Service (GPRS), Enhanced Data Rates for GSM Evolution (EDGE), GSM and High Speed Packet Access (HSPA) with the following characteristics:

- International Mobile Equipment Identifier (IMEI) – this is a unique 15 digit code used to identify a GSM cell phone to its network and is found on the compliance plate. This code also identifies manufacturer, model type, and country of approval of a handset.
- Subscriber Identity Module (SIM): There will be at least one slot for this card usually found under the battery panel. The face of this card may also contain the name of the network in which the SIM is registered.

- Integrated Circuit Card Identification (ICCID): This is an 18 - 20 digit number (10 bytes) imprinted on the face of the SIM. This number uniquely identifies each SIM. This number is tied to the IMSI which is associated to the IMEI when a handset is registered to a GSM network.
- International Mobile Subscriber Identity (IMSI): This number is typically a 15 digit number (56 bits) that consists of three parts, stored electronically in the SIM:
  - Mobile Country Code (MCC)
  - Mobile Network Code (MNC)
  - Mobile Station Identification Number (MSIN)

iDEN is a proprietary variant of TDMA/GSM network developed by Motorola. iDEN devices have the same characteristics of a GSM device with the additional ability of push-to-talk, a two-way radio system.

- Direct Connect Number /Radio-Private ID/MOTOTalk ID/iDEN Number: iDEN use a number based on the following format for communicating device-to-device: 012*345*67890.
  - The first three digits (012) make up the Area ID (region of your home carrier's network).
  - The next three digits (345) define the Network ID (specific iDEN Carrier such as Nextel, SouthernLink, Nii, MIKE/Telus, etc.)
  - Last five digits determine the Subscriber's ID (personal number from home carrier's network, sometimes the last five of the phone number).
  - The asterisk (*) is also part of this Direct Connect Number used as a separator to divide each of the aforementioned parts
- Subscriber Identity Module (SIM) is required by most GSM to successfully boot the phone. SIM is a smart card for all intents and purposes containing a 16-128KB electronically erasable programmable read-only memory (EEPROM). The SIM is assigned the cell phone number from the network which is tied to its ICCID, IMSI number as well as the IMEI number of the handset. [8]

Currently there are two types of data acquisition: logical and physical. Logical acquisitions are the most common type of acquisition and are performed with software such as Encase, FTK, etc. while physical acquisition allows you low level access to the device bypassing the device's security mechanisms.

2.1.1 Android

Android OS [7] is relatively new compared to other operating systems, initially released in the latter part of 2008. Over the next two and one-half years, there were six releases/updates to the Android OS which makes it harder to develop standards for data acquisition or forensic tools. In order to perform an acquisition an investigator must gain access to the OS memory through a process termed rooting. What rooting means is gaining access to the root directory (/) and having the appropriate permissions to take root actions within the device's OS. Some devices that run Android OS may require a third party application be installed on the mobile device to root the device. However, this would make any data recovered

inadmissible in court making an alternative way a priority. Once you have gained root access, the Android SDK shell will need to again be launched. Once in the shell, the dd command can be used to image the memory files using a command line interface. Although it may vary on the device, the file system is stored within the /dev/mtd directory in the following areas of interest:

- mtd0 handles miscellaneous tasks
- mtd1 holds a recovery image
- mtd2 contains the boot partition
- mtd3 contains system files
- mtd4 holds cache
- mtd5 holds user data

2.1.2 iPhone

iPhone OS has 3 primary domains: System, Local, & User; which correspond to the Core OS, Core Services, and the Application sub layer of the Cocoa Touch layer. The System domain contains all Apple installed software while on the contrary the User domain consists of all user files. The local domain includes the libraries and applications directories as well as OS specific applications. An investigator has to consider any possible options, which may include checking the iPhone firmware, mounting the iPhone in a Linux environment, or using the Apple Filing Protocol (AFP) to access the file system among other options. [8]

2.1.3 Blackberry

Unlike other operating systems, Blackberry has an extra option for messaging: PIN to PIN. Each Blackberry device is uniquely identified by an eight alphanumeric combination, known as a PIN. These messages are encrypted and can only be decrypted by another Blackberry device. PIN messages are not attached or associated with an email address resulting in different communications protocol from SMS and MMS messages which use TCP/IP and are not encrypted. Examining a Blackberry device, an investigator is required to create an interactive pager backup (IPD) file that contains a backup of the Blackberry device database. Any Blackberry device can be analyzed if not pin-protected. [8]

2.1.4 Windows Mobile

There isn't a preferred or standard method to forensically acquire data from a device with Windows Mobile OS. [6] Neither type of acquisition, logical or physical, will recover all relevant information from the mobile device. While a logical acquisition is better when acquiring active data, there is still a risk because RAM and flash memory is overwritten to establish an ActiveSync connection. ActiveSync is developed by Microsoft used to forensically acquire data from Windows Mobile O/S. It requires a dedicated .dll file that can be loaded onto the device under investigation. Logical acquisitions only provide a file system view only allowing an investigator to image the unallocated clusters that reside in active flash pages. Other disadvantages are that deleted data could be erased beyond recovery, expired flash blocks that still contain data won't be imaged, Active Wear Leveling, and Garbage Collection in the RAM. However, in some instances when a device is broken beyond repair or there is no standard interface

for forensics, a logical acquisition is not possible and a physical acquisition would be the next best option.

2.1.5 Symbian

Version 9.1 of Symbian's S60 platform [13] implemented a new security model that made it impossible to preserve the present state of a device running Symbian OS during forensic acquisition. This made it harder for an investigator to get a full memory image of the device and have to resort to methods similar to forensic acquisition on Windows Mobile Devices. Similar to Windows Mobile, it uses a connection agent but only if it is certified and properly signed. No open source tools are allowed due to the new security model.

2.2 Logical Acquisition

Logical acquisitions are those where forensic tools, commercial or open-source, are used and nothing is physically removed from the mobile device. The amount of extracted data varies with each individual device, but will usually include SMS, MMS, call registers, videos, pictures, audio files and calendar entries and tasks. Some forensic software will also include information that properly identifies the mobile device, such as make, model, ESN number off of the compliance plate, etc.

2.2.1 Internal Memory

What actually happens during a logical acquisition is that the forensic tool being used requests data from the phone, to which the phone responds and returns the requested data when it is available. [3] Once a device that's part of an investigation is properly seized, the device's state determines the next step. Whether the device is on or off is very important because if it is still on, an investigator can perform an acquisition with their tool of choice. However, if the device is off, it needs to stay off to prevent any changes to the device's memory and also prevent the device's security mechanisms from activating.

When performing data acquisitions each OS [8] has different things to consider or may require extra software to complete acquisition:

- Android OS [7] devices need to be rooted
  - permissions need to be given to the investigator for them to be able to take actions in the root directory of a device's memory
  - have an Android SDK available to run shell scripts to extract data
- iPhone OS
  - which may include checking the iPhone firmware
  - mounting the iPhone in a Linux environment
  - using the Apple Filing Protocol (AFP)
- Blackberry OS requires an investigator to create an interactive pager backup (IPD) file that contains a backup of the Blackberry device database. It also recommends having the following at an investigator's disposal:
  - Blackberry Desktop Manager - this tool is used to create the IPD file as well as restoring the IPD file into a BlackBerry simulator
  - Blackberry Simulator - specific to the model you are examining; allows the evidence IPD file to be viewed in a virtual environment
  - Software that can parse the IPD file and allow export to various formats

- Forensic Analysis Tool – Device Seizure, Encase, FTK, etc

When forensically analyzing a CDMA phone the internal memory is the main priority because unlike a GSM phone where SIM cards are required, it may or may not use a SIM card.

2.2.2 SIM

SIM [8] analysis is pertinent in the investigation of GSM/iDEN/hybrid CDMA/GSM devices because they can be placed in any unlocked device on the GSM network and can contain the following information that could be treated as evidence:

- Last Number Dialed (LDN)
- Phonebook/Contacts (ADN)
- Text Messages (SMS), including deleted text messages
- Location information (LOCI) from position of last usage
- Service Related Information

However the device state determines whether the SIM is analyzed first or last. If the device is on, SIM is analyzed after internal memory; otherwise, it is analyzed first. Ideally the original SIM should be cloned and use the cloned SIM inside the device during forensic analysis. The cloned SIM will not allow network access but will act similar to the original SIM. It is important to note that deleted SMS messages can only be extracted from SIM when it is not in a mobile device.

Taking these things into consideration will help the investigator get the most out of each acquisition because these considerations cater to each individual operating system.

2.3 Physical Acquisition

Physical acquisition is considered as a last resort because it involves a greater risk of damaging evidence on the device. Information retrieval can be achieved by either physically removing the flash memory chip, using a bootloader, or JTAG to extract data. [6] These methods all bypass any device security mechanism which gives you direct access to a device's memory. Through physical acquisitions, you view memory as hardware components view it, in its rawest form. Although you view the memory in its rawest form, the advantage is that you have limitless access to the phone's memory and not bounded by operating system restraints.

However to perform a physical acquisition, it requires special hardware outside of the forensic software. An investigator should be properly train doing such acquisitions using the following methods can be used:

1. Removing the memory chip from the device's circuit board
2. Access the JTAG access points, if they are any, to access the data.

After the data has been retrieved, a binary file known as a permanent memory (PM) file needs to be processed to a easier, more recognized, and readable format so that an investigator may be able to recover all data, viewable and deleted.

From an investigative point of view, a physical acquisition is more relevant to those mobile operating systems where a connection agent is used for a logical acquisition, such as Windows Mobile and Symbian, because it maybe more advantageous to perform a physical acquisition instead. Using a connection agent to perform a logical acquisition will limit the amount of data you retrieve from the device because of the operating system constraints. Windows Mobile uses Microsoft ActiveSync, which requires a dedicated .dll file that can be loaded onto the device under investigation. Logical acquisitions only provide a file system view only allowing an investigator to image the unallocated clusters that reside in active flash pages. Other disadvantages are that deleted data could be erased beyond recovery, expired flash blocks that still contain data won't be imaged, Active Wear Leveling, and Garbage Collection in the RAM. Unlike Windows Mobile OS, Symbian OS uses a connection agent also but only if it is certified and properly signed; no open source tools are allowed due to the new security model.

While this is a last resort for other operating system, it may be a viable option for those types of systems because you would have to perform both logical and physical acquisitions to get as much information as you can. However, in some instances when a device is broken beyond repair or there is no standard interface for forensics, a logical acquisition is not possible and a physical acquisition would be the next best option.

Considering these issues and taking them into preliminary consideration will help the investigator determine what needs to be done on site at the crime scene and what needs to be taken back to their labs for analyzing. Understanding how each operating system interacts with each tool will benefit an investigator to conduct a more efficient forensic analysis.

3. DIGITAL FORENSICS TOOLS

The convenience of mobile computing has become frustrating for the forensic community because it is harder to build tools that can be considered industry standard. Unlike computers, technologies for mobile devices are constantly advancing faster than any other technology. Device are advancing so quickly, that development for tools are not able to keep up because there are some drastic differences between forensics of computers and mobile devices as describe in the table below

3.1 Digital Forensics tools for Computers

Forensics for computers is easier and less complex in comparison to mobile devices. Computers have two types of memory: Random Access Memory (RAM), or secondary or volatile memory, and Read Only Memory (ROM), or primary memory. A mobile device only has one, RAM, unless a SIM card is present then the SIM card functions as ROM. The most popular operating systems for personal computers are: Windows, Mac, and UNIX, but there is a variety of manufacturers that produce mobile devices: RIM, Apple, Symbian, Palm, etc. just to name a few.

3.2 FTK Mobile Phone Examiner

FTK Mobile Phone Examiner (MPE) [1] is the most commonly used forensic tool for mobile devices in the US, a distinction

shared with Guidance's Encase Forensic suite. Mobile Phone Examiner can be used as a standalone application or as a fully integrated part of Forensic Toolkit (FTK) interface. Using MPE affords the investigator the option of a quick and easy field acquisition via cable, Infrared, or Bluetooth connection without altering data on the device, which is essential in establishing court admissible evidence. When integrated with FTK, MPE can take advantage of leading technology validated by courts and organizations such as Securities & Exchange Commission (SEC), Federal Bureau of Investigations (FBI), and the Internal Revenue Service (IRS) just to name a few. This integration would allow MPE to perform forensic analysis on multiple phones simultaneously within the same FTK interface as well as manipulate that data for easy interpretation. Reports produced by the integrated suite, which are instantly ready to be used as evidence in court, include both phone and computer analysis which allows an investigator to easily correlate data from a mobile phone to evidentiary data from a computer or another phone.

3.3 Oxygen Forensic Suite

Oxygen Forensic Suite [10] is the tool of choice for many agencies in Europe, serving law enforcement, tax and customs, government authorities in Great Britain, Germany, Australia, Sweden, and Finland among others. Oxygen prides itself on its reputation of being able to extract unique information from a smartphone such as phone basic information and SIM-card data, contacts list, caller groups, speed dials, missed/outgoing/incoming calls, standard SMS/MMS/E-mail folders, custom SMS/MMS/E-mail folders, calendar events schedule, tasks, and text notes. However the features are not truly unique as all three tools can extract this information. However Oxygen's ability to tap into the LifeBlog and geotagging in Symbian OS in Nokia phones gives it an advantage over its competition. Unlike MPE or Device Seizure, a special agent application is used to perform forensic analysis combining the advantages of both logical and physical data acquisitions.

3.4 EnCase Neutrino

Guidance Software has become an industry leader on the strength of its product EnCase Forensic software, aside from AccessData's Forensic ToolKit (FTK), and has over 30,000 licensed users of EnCase®. Its customer base includes more than 100 of the Fortune 500 and over half of the top 50, including: Allstate, Chevron, Ford, General Electric, Honeywell, Mattel, Northrop Grumman, Pfizer, UnitedHealth Group, Viacom and Wachovia. As a complement to their award winning, industry leading forensic solution, EnCase Neutrino [4] is designed to provide the same technology and foundation for forensic investigations for mobile devices. Amidst all the wireless signal blocking technologies, EnCase boasts a claim that the WaveShield technology used in EnCase Neutrino is the only extensively tested technology, including within close proximity of cell towers, to ensure integrity of evidence and reliability for field acquisitions. When performing data acquisition, a phone wizard is launched that identifies the device and determines the correct USB cable for a forensically sound acquisition. Unlike other tools, data acquisition and analysis starts with the device's SIM, if present, and then continues to

the device. Neutrino's ability to obtain the device's serial number, cell tower location, manufacturer information among other information, shows why it is considered the de facto standard for forensic solutions.

3.5 Paraben's Device Seizure

Device Seizure has low minimum system requirements so it can run on any computer, new, old, or ancient. It can also add support and perform forensic analysis on unsupported phones if they come from supported manufacturers. Similar to MPE, but unlike Oxygen, Paraben's device seizure [11] can search through a phone's memory dump for crucial evidence. Device Seizure focuses on the physical level of acquisition because you can acquire more information with physical acquisition than logical.

3.6 Other Tools

There are many other free sources or commercial tools that are available for use in forensic investigations such as:

- **Palm dd (pdd)** [12], which is a spin off the UNIX dd, it is a windows based command-line tool that allows an investigator to complete a physical data acquisition from Palm OS handhelds. PDD creates two files; one file has device specific information and the other file contains the bit by bit image. These files can then be exported to different forensic tools, such as EnCase or Autopsy. However since this is a command-line tool, graphic libraries, report generation, and search facilities are not included in these files.
- **Pilot-Link** [12] can be used to retrieve an image of the RAM of a PDA device. Pilot Link is open source software developed within the Linux community to provide a communication bridge between a Linux host and Palm OS digital devices. It uses the HotSync protocol which allows Pilot-Link to logically acquire the devices contents that can then be analyzed by EnCase, HEX editor, or Palm OS Emulator. Unfortunately, it doesn't support hashing algorithms, making it harder to compare acquisitions for data integrity.
- **TULP2G is short for Telefoon Uitlees Programma, 2e.** It is used to recover evidence from handheld devices. Currently, available plug-ins are mainly targeted towards GSM phone examinations

4. RELATED WORK

A literature review found little to no papers, journal articles, or conference proceedings that focused on forensic analysis of more than two operating systems or forensic tools. Some standards and benchmarks available to traditional computer forensics were briefly mentioned in the introduction. In an evaluation of CFTL [9], the introduction of general benchmarks for timestamp-based digital forensics was discussed. NIST recently published another study, in October 2009, which revised standards for cell phone forensics using device model, SIM, and removable memory as benchmarks.

5. PROPOSED WORK

There are many free sources and commercial digital forensics tools for mobile devices. However, there are few comparisons and benchmarks available to guide investigator or students to choose those tools for their practical needs. This section will address those issues.

During the experimentation of this case study, we will use SIMfill [5], a tool created by the National Institute of Standards and Technology (NIST), to automatically generate the test data for this case study which will then be placed on each mobile device via USB cable connection. After the data has been transferred to each device, each forensic tool will perform a forensic data acquisition and the data acquired documented. This process will be repeated two more times to ensure consistency and accuracy of the data being acquired and to satisfy the Federal Rules of Evidence [2]. Once the process is complete, we will compare the results based upon the following:

- Time it takes to acquire data
- The type of data acquired against the test set
- Categorically
  - By device model
  - By forensics tool
- How admissible is it as evidence

The data types we hope to establish benchmarks for include but are not limited to the following: images, messages (SMS, MMS, E-Mail), Call logs, deleted data, memory dump recovery, network traffic, etc. These particular data types were not subjectively chosen, but chosen according to common features that most forensic tools, commercial and open-source, list as retrievable information by their respective software. There will be two benchmarks set, one based on each benchmark category, forensic tool and operating system. A factor such as time could play just as much of a factor as the forensic tool being used or the operating system being used by the device and vice versa.

Through this exploratory experimentation, we will be able to give substantial detail to back up a claim of which investigation tool is optimal for various mobile devices.

6. CONCLUSIONS

Law enforcement agencies want to process all evidence as quickly and efficiently as possible, while also getting all important information for their investigation. Through this case study, we hope to start the process of creating some benchmarks for mobile forensics by modifying those already in place for computer & network forensics and adapting them to the mobile environment that we live in.

We would make the set of benchmarks available for any researcher who wants to compare the new tools with other tools for different operating systems. In the future we hope to improve on existing benchmarks and continuously retrieve various feedbacks to make benchmarks more effective and easy to use.

ACKNOWLEDGMENTS

This work has been supported in part by U.S. Department of Education grant P120A080094 and P120A090122.

REFERENCES

- [1] AccessData. (n.d.). *Mobile Phone Examiner*. Retrieved May 15, 2010, from AccessData: <http://www.accessdata.com/mobilephoneexaminer.html>
- [2] AccessData. (n.d.). *The Rules of Digital Evidence and AccessData Technology*. Retrieved May 10, 2010, from AccessData Corporation: http://accessdata.com/downloads/media/Rules_of_Digital_Evidence_and_AccessData_Technology.pdf
- [3] Curran, K. R. (2010). Mobile Phone Forensic Analysis. *International Journal of Digital Crime and Forensics*.
- [4] Gloe, T., & Bohme, R. (2010). The 'Dresden Image Database' for Benchmarking Digital Image Forensics. *SAC'10*. Sierre: ACM.
- [5] Guidance Software. (n.d.). *EnCase Neutrino*. Retrieved May 28, 2010, from Guidance Software: http://www.guidancesoftware.com/product.aspx?B=Product&Product_S=AccordianTwo&menu_id=117&id=348&terms=mobile+devices
- [6] Jansen, W., & Delaitre, A. (n.d.). *Mobile Forensic Reference Materials: A Methodology and Reification*. Retrieved from National Institute of Standards and Technology: <http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf>
- [7] Klaver, C. (2010). Windows Mobile Advanced Forensics. *Elsevier*.
- [8] Lessard, J., & Kessler, G. C. (2010). Android Forensics: Simplifying Cell Phone Examinations. *Small Scale Digital Device Forensics Journal*.
- [9] Mislán, R. (2008). Mobile Device Analysis. *Small Scale Digital Device Forensics Journal*.
- [10] Olsson, J., & Martin, B. (2009). Computer Forensic Timeline visualization tool. *Elsevier*, S78-S87.
- [11] Oxygen Forensic. (n.d.). *Oxygen Forensic Suite 2010*. Retrieved May 15, 2010, from Oxygen Forensic: <http://www.oxygen-forensic.com>
- [12] Paraben Corporation. (n.d.). *Device Seizure*. Retrieved May 29, 2010, from Paraben Corporation: <http://www.paraben-forensics.com/device-seizure.html>
- [13] Sansurooah, K. (2007). An overview and examination of digital PDA devices under forensics toolkits. *Proceedings of the 5th Australian Digital Forensics Conference* (pp. 34-51). Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.
- [14] Savoldi, A., Gubian, P., & Echizen, I. (2009). A comparison between Windows Mobile and Symbian S60 Embedded Forensics. *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 546-550). IEEE Computer Society.