EFFICIENT FORENSIC TOOLS FOR HANDHELD DEVICES: A COMPREHENSIVE PERSPECTIVE

Somasheker Akkaladevi[1]
[1] Virginia State University
Department of Computer Information Systems
Petersburg, Virginia 23806, USA
sakkaladevi@vsu.edu

Himabindu Keesara[2]
[2]Texas A&M University - Corpus Christi
Department of Computing Sciences
Corpus Christi, Texas 78412, USA
bindukeesara@yahoo.com

Xin Luo[1]
[1] Virginia State University
Department of Computer Information Systems
Petersburg, Virginia 23806, USA
xluo@vsu.edu

ABSTRACT

With the continued growth of the handheld device market, it is possible that their use in criminal activity will only continue to increase. These gadgets are compact hybrid devices integrating the capabilities of Personal Digital Assistant (PDA), mobile phone, camera, music player, FM radio, Global Positioning System (GPS) and so on. These devices have become common during the past few years. The rapid technological advancements and increasing popularity of mobile devices pose great challenges for investigators and law enforcement officials all over the world. The methodology and approach one uses in a digital forensics investigation is crucial to the outcome of such an investigation. In this paper, we present an overview of forensic tools and discuss the challenges involved in the design of forensic tools with the steps needed to develop better toolkits in the digital forensic world.

INTRODUCTION

Information security has become a mission-critical component of today’s society. Ineffective analysis of security threats can result in unpredictable catastrophes. The emergence of information forensics comes from the incidence of criminal, illegal and inappropriate behaviors. In general, the role of forensics can be classified in the following areas:

1. To facilitate investigations of criminal activities using forensic methodologies, techniques and investigation models.
2. To preserve, gather, analyze and provide scientific and technical evidences for the criminal or civil courts of law.
3. To prepare proper documentations tied to law enforcement.

The field of digital forensics has long been centered on traditional media such as hard drives. Being the most common digital storage device in distribution it is easy to see how these devices had become a primary point of evidence. However, as technology brings digital storage to more and more devices, forensic examiners need to prepare for a change in what types of devices hold a digital fingerprint. Cell phones and PDA (Personal Digital Assistant) devices are so common that they have become standard in today's digital examinations.

Handheld devices store personal information, voice calls, and contact information that provides digital evidence during an investigation (Patterson, 2004). Forensic examiners have to follow clear, well-defined methodologies and procedures for proper retrieval and speedy examination of information present on the device (COMPUTER FORENSICS, 2007).

Cell phones are designed for mobility, they are compact in size, battery powered, and lightweight, often use registered operating systems, a Subscriber Identity Module (SIM), and a removal media. Cell phones operate on platforms like RIM (Research in Motion), Pocket PC and Palm OS devices. SIM uniquely identifies the subscriber, determines the phone number, and contains the algorithms needed to authenticate a subscriber to a network. A user can remove the SIM from one phone, insert it into another compatible phone, and resume use without the need to involve the network operator (Mellars, 2004). The hierarchically organized file system of a SIM is used to store names and phone numbers, sent and received text messages, and network configuration information. Cell phones are becoming so advanced that by using them it is possible to perform various functions such as browsing, email communication, and storing files (Ayers, 2004).

Handheld devices are rooted in their own operating systems, file systems, file formats, and methods of communication. Dealing with these devices creates unique problems for examiners. Performing a forensic exam on a cell phone or PDA requires special software and special knowledge of the way these devices work, as well as where possible evidence could be stored.

PDAs differ in several important ways compared with personal computers (PCs). PDA's vary in areas of Operating System, interface style and hardware components and they work with different operating systems such as Linux, Palm OS, and Microsoft Pocket PC. A PDA basically contains a processor, RAM, ROM and other ports to connect it to a computer (Valli, 2005). The ROM stores the operating system of the PDA and information which should not be altered, whereas the RAM stores the handler's data and works with battery power whose failure causes the information to be lost. Compact flash and secure digital slots assist cards of memory and wireless communication. Users mainly use PDAs for storing data in various file formats, access the Internet, send and receive emails (Jansen, 2004). PDA's have personal information management (PIM) applications that consists of calendar, task management, contacts and e-mail software. PDAs can be synchronized with a personal computer (PC) by using software such as Microsoft Pocket PC ActiveSync, HotSync from Palm etc. Due to the design and architecture, PDAs require specialized forensic tools and procedures which are distinct from tools used for single PC systems and network servers.

Previously hackers used to attack PCs and servers of organizations to destroy the data. With users using more and more handheld devices, now the problem of hacking, viruses, Trojans, worms have spread to these devices. Hackers now hack these devices, or use these devices instead of a computer to hack these devices or other computers. Therefore there exists a need for having forensic tools for these devices apart from having them for computers.

When handheld devices are involved in a crime, forensic examiners need tools to properly retrieve and analyze data present on the device. In this article, we tend to present a comprehensive perspective on a variety of forensic tools which respectively has its own advantages and limitations. Section 2 presents a few forensic tools for PDAs and Mobile phones which are available in the market. We also provide directions for future research in the area of forensic toolkits development and implementations.

FORENSIC TOOLKITS

Forensic examiners have to conduct well-defined procedures when dealing with digital handheld devices and various removable media's (COMPUTER FORENSICS, 2007). Physical or logical acquisition is used by forensic tools to obtain information. Physical acquisition easily imports images of physical devices into another tool for reporting and allows examining of unused file system space; whereas logical acquisition gives a natural and understandable structure of acquired information. Physical acquisition denotes a complete copy of the RAM, while logical acquisition denotes a full copy of objects such as files and directories. It is better to do both types of acquisition, as physical acquisition memory enables us to examine the processor and other hardware related components and logical acquisition memory enables us to examine a process through the operating system facilities (Patterson, 2004).

Forensic examiners have to prepare a bit-by-bit copy of the content present in digital device, test the copy to retrieve information and analyze the retrieved information to document. The handheld devices differ in design, they require specialized forensic tools distinct from those tools used for PC (AYERS, 2007) and these can't be directly seized because they are flexible, and use volatile memory against non-volatile memory to store handler's data, such that loss of battery power results in loss of data. When the forensic examiner is dealing with these portable digital handheld devices the tool selected must acquire the content of the device, recover deleted information, e-mail message information, find the visited websites, display graphic file formats, text images, files stored on removable media, obtain user's passwords and recognize file types by header information. Section 3 further discusses about the various forensic tools available for these devices.

FORENSIC TOOLKITS FOR PDAS

The range of tools available for PDA's is limited and only a couple of tools assist the forensic examiner's with a full range of examination, organization, acquisition, reporting and documenting functions whereas the remaining tools focus on a single function (Valli, 2005).

The tools available for the forensic examiner to investigate a crime when a PDA is involved are PDA Seizure, EnCase, Palm dd (pdd), Pilot-lint, and other miscellaneous tools. All these tools are not applicable for each and every operating system for PDAs; they are narrowed to Pocket PC and Palm OS. Table 1 lists the tools and services provided for each operating system of PDA's.

Tool	**POCKET PC**	**LINUX**	**PALMOS**
Pilot-link	Not valid	Not valid	Acquisition
Palm dd	Not valid	Not valid	Acquisition

PDA Seizure	Acquisition, Reporting,	Not valid	Acquisition, Reporting, Examination
EnCase	Not valid	Reporting, Examination	Acquisition, Reporting, Examination

Table 1. PDA Forensic Tools

ENCASE

This is the most popular forensic software toolkit. Some of the various features supported by this toolkit are analytical tools, suspect media acquisition, data capture, documentation and search features. EnCase doesn't support Pocket PC devices, although it is a very familiar tool for PCs and Palm OS devices. A complete physical bit-stream image of Palm OS devices is created and this bit-stream image is checked with the already obtained existing CRC (Cyclical Redundancy Checksum) values. This process yields an EnCase evidence file which is created as a read-only file. From here the software rebuilds the file structure using the logical data in the bit-stream image (Jansen, 2004). The forensic examiner can then look over the device content to trace for any evidence without the original data being getting manipulated.

EnCase includes features like bookmarking and reporting. Bookmarking allows files, folders, or sections of a file to be highlighted and saved for later reference. Each case is bookmarked and is saved in case files. Any data can be bookmarked for future reference. The forensic examiners can utilize the reporting feature of EnCase and can then search for information of one file, two files, multiple files, all the files in the case etc. The examiner can also obtain a report of the entire case file that is created.

PDA SEIZURE

PDA seizure is another forensic software toolkit to obtain and examine the data on PDAs. This tool can only produce a forensic image of Palm OS and Pocket PC devices. PDA seizure searches acquired files for data and generates a report of the findings (Jansen, 2004). Similar to EnCase, PDA Seizure also includes the capability to bookmark and organize information. The graphics library provides the functionality of automatic collection of images according to their file extensions.

Data can only be acquired from the Palm OS device when in console mode. The logical data can be obtained once the image or screen shot of the memory of the Palm device is obtained. This logical data can be obtained in two ways; either through HotSync or through physical acquisition of the RAM image file. The obtained information can then be used by the forensic examiners to trace the sources of attack.

PALM DD (PDD)

The Palm dd (pdd) tool runs only on Windows based systems and is mainly used by forensic examiners for physical acquisition (Frichot, 2004). Palm dd has no GUI support and everything has to be done from the command prompt of Windows. The tool also lacks support for bookmarking, search capability, and report generation.

A complete copy of the device's memory is acquired during the acquisition stage, and the data retrieved by pdd includes all user applications and databases. Two files are generated from the information obtained. One file is a text file which has all the information pertaining to the Palm device in investigation (Grant, 2002). The other file is created from the output sent by the user. Both these files contain an image copy of the Palm device. The forensic examiner can then inspect these two files to find any evidence. The tool also provides support for importing the files generated by pdd to EnCase tool for other forensic analysis on these files not supported by pdd.

FORENSIC TOOLKITS FOR CELL PHONES

Cell phones are not limited to just phone calls but they provide lots of functions such as accessing the Internet, sending and receiving emails, sharing photos on the web, access to a calendar similar to that available on windows for organizing information, and also as a small storage device for storing important data and files. Basic phones can store and process personal information without a desktop or notebook computer. Many tools are available for cell phones for performing forensic analysis, but these tools are not always compatible with all the manufacturers and different models of cell phones (FORENSICS, 2007). These tools can obtain data from these phones in a variety of ways such as IrDA (Infrared Data Association), through a USB connection, by Bluetooth, or by a serial cable connected to a computer (Mellars, 2004). Tools can acquire a wide range of information that includes PIM (Personal Information Management) data, SMS/EMS/MMS messages, logs of phone calls; email, IM content; URLs and content of visited Web sites; audio, video, and image content; SIM content; and uninterrupted image data. Table 2 lists the tools and facilities provided for certain types of cell phones.

SIMs can be removed from a phone and read using a specialized SIM card reader and software. A SIM can also be placed in a standard-size smart card adapter and read using a conventional smart card reader (AYERS, 2007). Table 3 lists several SIM forensic software tools.

Tools	Functions	Features
Cell seizure	Acquisition, Reporting, Examination	- Targets certain models of GSM, TDMA, and CDMA phones - Internal and external SIM support - Only cable interface is supported
GSM .XRY	Acquisition, Reporting, Examination	- Targets certain models of GSM phones - Internal and external SIM support - Cable, Bluetooth, and IR interfaces are supported
MOBILedit! Forensic	Acquisition, Reporting, Examination	- Targets certain models of GSM phones - Internal and external SIM support - Cable and IR interfaces are supported
BitPIM	Acquisition, Examination	- Targets certain models of CDMA phones - Recovering of SIM information is not supported

Table 2. Cell Phone Tools

Tools	Functions	Features
SIMIS	Acquisition, Reporting, Examination	Only external SIM cards are supported
ForensicSIM	Acquisition, Reporting, Examination	Only external SIM cards are supported Produces physical facsimiles of SIM for defense and prosecutor, and used as a storage record
Forensic Card Reader	Acquisition, Reporting	Only external SIM cards are supported
SIMCon	Acquisition, Reporting, Examination	Only external SIM cards are supported

Table 3. SIM Tools

CELL SEIZURE

Cell Seizure is a forensic software toolkit for acquiring, searching, examining, and reporting (Ayers, 2004) data associated with cell phones operating over CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), and GSM (Global System for Mobile communication) networks. By using Cell Seizure software data can be acquired from cell phones, but a proper cable must be selected from either the Cell Seizure Toolbox or a compatible cable to establish a data-link between the phone and the forensic workstation. Cell Seizure features include bookmarking, automatic assembling of found images under a single facility and searching. The following data can be obtained on most cell phones with the tool:

- SMS History: Inbox/Outbox
- Phonebook: SIM-Card, Own Numbers, Speed Dialing, Fixed Dialing
- Call Logs: Dialed Numbers, Received Calls, Missed Calls
- Calendar: Reminder, Meeting, Memo
- Graphics: Wallpaper, Picture Camera Images, EMS Template Images
- WAP: WAP Settings, WAP Bookmarks
- SIM: GSM Specific data

MOBILEDIT!

MOBILedit! is a forensic application that allows examiners to acquire logically, search, examine and report data from CDMA (Code Division Multiple Access), PCS (Personal Communications Services), and GSM (Global System for Mobile communication) cell phones. The tool (AYERS, 2007) connects to cell phone devices through an Infrared (IR) port, a Bluetooth link, or a cable interface. Once the connection is established, the phone model is identified by its manufacturer, model number, serial number and a corresponding picture of the phone. The data acquired from the cell phone is stored in a .med file format. After a successful acquisition, the following fields are populated with data: Subscriber information, Device specifics, Phonebook, SIM Phonebook, Missed calls, Last Numbers Dialed, Received Calls, Inbox, Sent Items, Drafts, Files folder. Items present in the Files folder, range from Graphics files to Camera Photos and Tones, and depend on the phone's capabilities. MOBILedit! features include myPhoneSafe.com service, which provides access to the IMEI (International Mobile Equipment Identity) database to register and check for stolen phones.

FORENSICSIM

Radio Tactic's ForensicSIM toolkit components include: acquisition terminal, analysis application, control card, data storage cards and the card reader (Ayers, 2004). The toolkit deals with acquisition of data and analysis of data. Acquisition of data is carried out using the acquisition terminal which is a stand-alone unit that guides the examiner through each step of the acquisition process. Analysis of data is carried out using the ForensicSIM card reader, attached to a PC running the ForensicSIM analysis application. Examiners use a control card to access the acquisition terminal and to prevent unauthorized use.

The terminal's primary function is to capture copies of the data from the target SIM to a set of data storage cards. ForensicSIM toolkit allows examiners read-only access to SIMs and generates textual reports based on the acquired content. Reports can be viewed internally, saved to disk, or printed for presentation purposes.

FORENSIC CARD READER

The Forensic Card Reader (FCR) consists of FCR software that allows the examiners to acquire data from SIM cards without modification and a smart card reader with USB connection. The tool (AYERS, 2007) allows the examiner to select specific data elements that can be later stored and displayed in a finalized report. Operations details like case number, evidence number, and examiner information can be automatically merged into the report. All data elements like phone directory, abbreviated dialing numbers, fixed dialing numbers, SMS messages, identifiers of the SIM, deleted SMS messages are acquired.

The tool stores a complete report in an XML format. Extended phone book entries, including additional numbers and email addresses can be acquired. The supplied FCR reader allows examiners to use either small or large SIM cards without the need for an adapter. SIM cards for GSM mobiles and also SIM cards for 3G mobiles can be used with FCR.

CHALLENGES IN HANDHELD FORENSICS AND THE NEXT STEPS IN THE FORENSIC TOOLKIT DEVELOPMENT

Handheld devices turn out to be quite challenging for forensic investigations, primarily because of their compact size, integrated features and the availability of a wide range of models and accessories. In this section we describe the challenges involved in designing forensic tools and the work that needs to be carried out in order to develop better forensic toolkits.

<u>Data storage differences:</u> Unlike computers, mobile devices do not have hard disks. They generally store data in volatile memory, which will be lost if there is no adequate power. Recovering volatile evidence and analyzing it could turn out to be a tedious task. Resetting the

device accidentally while examining may result in the loss of data. A hard reset will wipe out everything from RAM. A soft reset reinitializes the dynamic memory and records marked for deletion are removed. Loss of battery life causes a hard reset and hence the battery level needs to be continuously monitored. Most Windows mobile devices support additional memory devices like MMC, SD and CF cards. It is essential to search and seize such associated memory device.

State of the device: Even if a device appears to be in off state, it may not be entirely inactive, as background processes may be running. A sudden transition from one state to another may result in loss of data. Care should be taken to store the current state of the device using hashing or various cryptographic techniques. The device under investigation may contain malicious software like a virus or a Trojan. Toolkits need to consider the possibility of such malicious programs and avoid the possibility of viruses or Trojans spreading over other devices either over a wired or wireless interface.

Hardware and OS version differences: The forensic investigator may come across different types of hardware during an investigation. The models may be different in their size, technical specifications and features. The version of the operating system may also differ. Tools applicable to a particular version and model may not work well with another.

Exploiting the system possibilities: If the device is password protected, the forensic investigator needs to gain access to the device without damaging the device or the data. Different techniques such as exploiting system vulnerabilities, authentication weaknesses and gaining access through backdoor can be used. Toolkits should also consider the possibility of different mechanisms which can be used by the suspects to alter the data in the handheld devices using encryption and other techniques.

Currently offered tools or data analysis techniques do not scale properly to the networked environment. Most tools and data analysis techniques assume the analysis or imaging of a single computer, offline from the network environment. Tools will need to address the impact of data integrity and transport issues when collecting information across the network.

Handheld devices are designed differently. They might have items associated or attached to them that have file systems, like media cards. The tools the examiner uses must understand not only the operating system on the device that chooses how the data is stored, but also the design of the device to the chip set level to gauge how much storage is available on the device. Beyond this, the tool must understand how to communicate with the device in order to gain access at a low level to acquire all data available on that device for evaluation.

Handheld forensics needs to acquire active memory image unlike traditional bitstream image. Active memory image is similar to a bitstream image as it is copying allocated and unallocated data (Chen, 2005). Where it differs from a traditional bitstream image is that there is more data available on the device either reserved by the manufacturer or encrypted and locked from access, making it inaccessible to the examiner.

Traditionally forensic toolkits lack the performance speed in the investigation process. For example traditional approach is to utilize a single workstation to perform digital investigation against a single source media which is time-consuming (Patterson, 2004). As the media storage capacities are increasing, investigation using a single workstation lacks performance. Toolkit development should consider high performance computing using more than one computer and more sophisticated data analysis techniques to meet the challenges of massive amounts of data on storage devices. They need to scale up machine resources to match the growth of the forensic targets. Since most current digital forensics operations, such as computing cryptographic hashes, thumbnail generation, file carving, and string searches are I/O-bound, the performance of existing investigative tools will become completely unacceptable as the size of the problem (determined by capacity) grows significantly faster than the ability to process it (determined by drive latency and transfer rate limitations).

To improve the CPU-intensive operations performance toolkits need to employ implementations to get more from the current hardware platforms or enable the use of more machine resources in a distributed fashion. For example in a distributed computing environment we can distribute the digital evidence file over a cluster.

Files should be spread in a fashion which enables many files in RAM during processing, and these files should be distributed to all the computing nodes. DELV (Distributed Environment for Large-scale investigations) provides a look at how distributed systems can be applied to digital forensics (Roussev, 2004).

Analyzing the data from a handheld storage media can take more time. For the purpose of quickly restoring operations, an operating system hash library could be constructed to fingerprint hash values of operating system files. A quick comparison of this hash list to the fingerprint obtained from a suspect system could yield important information in the event of a crime scene.

Some digital forensics operations straddle the machine vs. human scalability line. Sophisticated image analysis is one example, where deeper analysis of images can save a significant amount of human effort, but the analysis may only be feasible if sufficient computational resources can be applied.

To design better forensic toolkits we need to perform work that allows us to detect data hidden within the network traffic. For this purpose we need to extract data hidden in processing data transactions or streaming media. We need to look at the hidden data area which looks legitimate or harmless but hidden within the bits of another message which is the true message.

Another effective and easy solution to improve the performance is to consider only the relevant data and systems for the investigation process. Getting the relevant data for the investigation is always a difficult task.

Sometimes a single tool may not perform all the necessary functions. So in many cases, a combination of tools needs to be used. Investigators need to evaluate the possibilities of the toolkit combinations for the specific investigation process. It is also important for any forensic toolkit to support Multilingual Digital Forensic processing capability. Since these devices are extremely compact, there is every possibility of them being involved in crimes, which can easily cross geographical boundaries. In developing such toolkits we need to use mechanisms to include multilingual information retrieval, focusing on the problem of searching, sorting, classifying, and organizing information in many different languages.

CONCLUSION

This paper presents a comprehensive overview of some prevalent software tools available for examining PDAs and Cell phones which are useful in any Digital Forensic Investigation. As digital technology evolves, new versions of tools for forensic examination of PDAs and Cellular devices also continue to improve. Before being used, forensic examiners have to understand the functionality and scope of these tools. When choosing a tool different criteria’s are to be considered like their quality, capability, affordability, usability, and accuracy. Examiners should have the documentation of the functionality of a tool to help them at the time of investigation. PDA forensic tools are a relatively recent development and in their early stages of maturity. New toolkits designed with the proposed guidelines using different architectures keeping the performance measures can be expected to improve and therefore meet investigative requirements. The development of forensic software must evolve with technological advances in handheld devices, allowing data from these devices to be acquired.

REFERENCES

AYERS. (2007). *An Overview of Cell Phone Forensic Tools.* http://www.techsec.com/TF-2006-PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf.

Ayers, R. J. (2004). Cell Phone Forensic Tools: An Overview and Analysis. *NIST Interagency Reports* .

Chen, Y. R. (2005). Content-based image retrieval for digital forensics. *In Proceedings of the First International Conference on Digital Forensics.*

COMPUTER FORENSICS. (2007). Retrieved from Mobile and PDA Forensics: http://www.forensics.nl/mobile-pda-Forensics

FORENSICS. (2007). Retrieved from Mobile Phone Forensics: http://www.mobilephoneforensics.com/why-mobile-phone-forensics.php

Frichot, C. (2004). Analysis of the Integrity of Palm Images Acquired with PDD. *2nd Australian Computer, Information and Network Forensics Conference.* Perth, Western Australia.

Grant, J. (2002). *Pdd: Memory Imaging and Forensic Analysis of Palm OS Devices.* Retrieved from http://www.grandideastudio.com/files/security/mobile/pdd_palm_forensics.pdf

Jansen W., A. R. (2004). *Guidelines on PDA Forensics.* Retrieved from http://csrc.nist.gov/publications/nistpubs/80072/sp80072.pdf

Mellars, B. (2004). Forensic Examination of Moblie Phones. Digital Investigation. *The International Journal of Digital Forensics & Incident Response* , 1(4), 266-272.

Patterson, D. (2004). eForensic Solutions: Cell Site Analysis. *Latency lags bandwith, Communications of the ACM,* (pp. v.47 n.10, p.71-75,).

Roussev V., R. G. (2004). Breaking the performance wall: The case for distributed digital forensics. *In Proceedings of the 2004 Digital Forensics Research Workshop.*

Valli, C. (2005). Issues relating to the Forensics Analysis of PDA and Telephony (PDAT) enabled devices. *ECIW 2005: 4th European Conference on Information Warfare*. University of Glamorgan, UK Wales, MCIL.