Mobile Device Forensics in Academia

How we find out what we need to find out.
Mobile Device Forensics in Academia

Richard P. Mislan, PhD
Assistant Professor
Department of Computing Security

Rochester Institute of Technology
B. Thomas Golisano College of Computing and Information Sciences
152 Lomb Memorial Drive
Rochester, NY 14623-5603
Phone: 585-475-2801 Fax: 585-475-2181
rick.mislan@rit.edu
Academia

ac·a·de·mi·a /ˌakə'dēmēə/
Noun. Origin 1945–50; Neo-Latin

the environment concerned with the pursuit of Research, Education, and Scholarship.
"Study the past if you would define the future...."

- Confucius
In 2002...
Forensic Examination of a RIM (BlackBerry) Wireless Device

June, 2002

Error: Condition. Rewrite to 1's only in 63K blocks.

Rewrite: Save 64K block to SRAM, erase 64K block of write back to erased Flash block. This takes approximately ...

It goes without saying that the hardware is optimized for the best use of the hardware available by implementing a log writen as a linked list one at a time, each entry appended to the list of the "old end log". Each file or record has its own unique identifier, a number between 0 and 65536.

When a change is necessary to an existing record, the original record is marked as dirty (but sealing most likely) and the new version is written to the end of the file system with a new unique identifier. This process eliminates the need for on-the-fly erasures which cost a great deal of time. Periodically, the OS will clean old records marked as dirty, and defragment the file system, if necessary, to allow for more room for the file system to grow (expand the log). Once the end of address space is reached, the log wraps back around to the beginning of the address space. Unlike traditional file systems, fragmentation occurs as one direction only. Even if the first part of a file is near the end of address space and the second part wraps back around to the beginning, the virtual address space is the log, which is in one direction only.

1. Email 1 is received and written to the file system
2. Email 2 is received and appended to the file system
3. Item is added to the calendar and is appended to the file system
4. Email 2 is deleted
5. File system cleanup occurs at next reset or when out of space

The log based file system and its interaction with the standard applications has notable ramifications when it comes to recovering whole files that either cross 64K sector boundaries or for which storage has been written several times. Take for instance the case of receiving a large email.
WHEN PALM WAS KING
pdd: Memory Imaging and Forensic Analysis of Palm OS Devices

Joe Grand
jgrand@mindspring.com

Abstract
One goal of incident response is to preserve the entire digital crime scene with minimal or no modification of data. This paper introduces pdd or “Palm dd”, a Windows-based tool for memory imaging and forensic acquisition of data from the Palm operating system (OS) family of Personal Digital Assistants (PDAs). pdd will preserve the crime scene by obtaining a bit-for-bit image or “snapshot” of the Palm device’s memory contents. Such data can be used by forensic investigators, incident response teams, and criminal and civil prosecutors.

This paper also presents the Palm OS internals (hardware, file system, and debugger functionality), pdd details¹ (usage, process, flowchart, and timing), and forensic analysis results (flash memory, record removal and deletion, retrieval of system passwords, and telephony application).

1 Introduction
PDAs are ubiquitous in the consumer marketplace and it is only natural that they will, as desktop and laptop computers have, become a target for criminal investigations and forensic analysis. pdd or other tools that aid in data acquisition and analysis of portable devices should be readily available in any incident response toolkit, as should any tool that maximizes an investigator’s ability to collect credible digital evidence.

The Palm OS has been licensed to a number of vendors including Handspring, Sony, IBM, Kyocera, Samsung, QUALCOMM, Franklin Covey, TRG, and Symbol Technologies. Devices running Palm OS own nearly 80 percent of the global handheld computing market², equal to approximately 20 million devices, and consist of consumer-based PDAs, telephones integrated with PDA functionality, and barcode and wireless integration for industrial applications. pdd has been designed to work with all devices running Palm OS.

²The examples and descriptions of pdd are for release version 1.1 and may change as the tool is updated.

© 2002 John Wiley & Sons, Inc.
2 years later...

2004
Rick Ayers & Wayne Jansen

August 2004

Guidelines on PDA Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

PDA Forensic Tools: An Overview and Analysis

Rick Ayers
Wayne Jansen

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-72
Sponsored by the Department of Homeland Security

NISTIR 7100

National Institute of Standards and Technology
U.S. Department of Commerce
Tools and Operating Systems – THEN...

<table>
<thead>
<tr>
<th>PDA SEIZURE OUTCOME – POCKET PC</th>
<th>36</th>
</tr>
</thead>
<tbody>
<tr>
<td>JORNADA 548</td>
<td>36</td>
</tr>
<tr>
<td>IPAQ 3875/3970/5455</td>
<td>37</td>
</tr>
<tr>
<td>PDA SEIZURE OUTCOME - PALM OS</td>
<td>40</td>
</tr>
<tr>
<td>PALM III/PALM Vx</td>
<td>40</td>
</tr>
<tr>
<td>VISOR PLATINUM</td>
<td>41</td>
</tr>
<tr>
<td>TUNGSTEN C</td>
<td>42</td>
</tr>
<tr>
<td>ENCASE OUTCOME - PALM OS</td>
<td>44</td>
</tr>
<tr>
<td>PALM III</td>
<td>44</td>
</tr>
<tr>
<td>PALM Vx</td>
<td>45</td>
</tr>
<tr>
<td>VISOR PLATINUM</td>
<td>46</td>
</tr>
<tr>
<td>TUNGSTEN C</td>
<td>47</td>
</tr>
<tr>
<td>REMOVABLE MEDIA</td>
<td>48</td>
</tr>
<tr>
<td>ENCASE OUTCOME - LINUX</td>
<td>49</td>
</tr>
<tr>
<td>ZAURUS SL-5000</td>
<td>49</td>
</tr>
<tr>
<td>DD OUTCOME - LINUX</td>
<td>51</td>
</tr>
<tr>
<td>ZAURUS SL-5000</td>
<td>52</td>
</tr>
<tr>
<td>IPAQ 3970</td>
<td>53</td>
</tr>
</tbody>
</table>
Forensic examination of mobile phones

Barrie Mellars

Digital Crime Unit, LGC, Queens Road, Middx, Teddington TW11 0LY, United Kingdom

KEYWORDS
Mobile phones; SIM cards; Cellular telephone network; Forensic investigation

Abstract The proliferation of mobile phones in society has led to a concomitant increase in their use in and connected to criminal activity. The examination and analysis of all telecommunications equipment has become an important aid to law enforcement in the investigation of crime. An understanding of the mechanism of the mobile phone network is vital to appreciate the worth of data retrieved during such an examination. This paper describes in principle the way a cellular mobile phone network operates and how the data is processed. In addition it discusses some of the tools available to examine mobile phones and SIM cards and some of their strengths and weaknesses. It also presents a short overview of the legal position of an analyst when examining a mobile phone.

© 2004 Elsevier Ltd. All rights reserved.
AT Commands
PART 2 COMPUTERS

CHAPTER 8 COMPUTER BASICS FOR DIGITAL INVESTIGATORS 193
9 APPLYING FORENSIC SCIENCE TO COMPUTERS 211
10 FORENSIC EXAMINATION OF WINDOWS SYSTEMS 255
11 FORENSIC EXAMINATION OF UNIX SYSTEMS 289
12 FORENSIC EXAMINATION OF MACINTOSH SYSTEMS 323
13 FORENSIC EXAMINATION OF HANDHELD DEVICES 337
Mobile Forensics in Academia

• SIMs
• Shielding
• SMS
• GPS
• Hashing
• Images/Videos
• Legal

• Operating Systems
  • Android
  • BlackBerry
  • iOS
  • Maemo
  • Symbian
  • WebOS
  • Windows
• Other…
Forensic analysis of mobile phone internal memory

Svein Y. Willassen
Norwegian University of Science and Technology

Abstract

Mobile phones have become a very important tool for personal communication. It is therefore of great importance that forensic investigators have possibilities to extract evidence items from mobile phones. Modern mobile phones store evidence items on SIM-cards as well as internal memories. With the advent of text-messaging, more and more of these items are examined of such memories, including the SIM until now.

This paper presents two different methods for imaging phone SIMs. The methods are applied to several different SIMs and the the can be utilized in practice. The discovery of mobile phone challenges the current mobile phone and

1.0 Introduction

It is clear that mobile phones contain items of interest in investigations. The mobile phone has become a tool for communication, and therefore frequently contains items of interest. Obtaining information on such activities is therefore important. The content of a mobile phone is therefore an important source of evidence.

This paper first examines what evidence items can be found on different methods for imaging phone SIMs. The content is examined for evidence items.

SIMCon - SIM Content Controller

SIMCon allows the user to securely image all files on a GSM SIM card to a computer file with a standard smart card reader. The user can subsequently analyze the contents of the card including stored numbers and text messages.

Some of SIMCon's features:
- Read all available files on a SIM card and store in an archive
- Analyze and interpret content of files including text messages and stored call logs
- Recover deleted text messages stored on the card but not readable
- Manage PN and PIN codes
- Write report that can be used on evidence based on selection of phone numbers
- Secure file archiving using hashing
- Export items to files that can be imported in popular spreadsheet programs

SIMCon is made for use within law enforcement and is an investigatory tool. SIMCon can however also be a valuable tool for other who need to secure evidence. The user can therefore obtain a free copy of SIMCon by sending an e-mail to SIMCon@nrc.no at the price of EUR 95.

Click here to see screenshots and features of SIMCon.
Click here to buy SIMCon now.
Click here to read more about mobile phone analysis on mobileforensics.com
Results of Field Testing Mobile Phone Shielding Devices

Eric Katz, Richard Mislav, Marcus Rogers, and Anthony Smith
Center for Education and Research Information Assurance and Security (CERIAS) and Purdue Cyber Forensics
Purdue University, West Lafayette IN 47907-2086, USA
ekatz@purdue.edu

Abstract. This paper is based on thesis research from the authors. Mobile phones are increasingly a source of evidence in criminal investigations. The evidence on a phone is volatile and can easily be overwritten or deleted. There are many devices that claim to radio isolate a phone in order to preserve evidence. There has been little published research on how well these devices work in the field despite the escalating importance of mobile phone forensics. The purpose of this study was to identify situations where the devices used to protect evidence on mobile phones can fail. These devices were tested using mobile phones from three of the largest services providers in the U.S. Calls were made to contact the isolated phones using voice, SMS, and MMS at varying distances from the provider’s towers. In the majority of the test cases the phones were not isolated from their networks.

Keywords: Mobile phones, forensics, shielding, radio isolation, thesis.

1 Introduction

Mobile phones have penetrated our society like few other technologies have. These phones are storing ever-increasing amounts of information about their owners. It is no surprise that mobile phones are now commonly seized as a source of evidence during
Falsifying SMS Messages

Thomas Marryat, John Corcoran

Abstract - Mobile telephone examiners are frequently asked to comment upon whether SMS messages presented in evidence are authentic. Throughout the years the devices have evolved and therefore the methods of data manipulation have also been adapted. This paper reviews the examination of the mobile telephone in the context of SMS messages and considers the methods that may be used to verify the authenticity of the SMS messages. The examination of the mobile telephone is performed to confirm that the report provides an accurate representation of the mobile telephone’s content; however, it is not always possible to determine if the SMS messages have been falsified on the phone itself.

An investigation was undertaken to establish whether it is possible to falsify SMS messages on a mobile telephone without access to privileged hardware or software. A common available flasher/service tool was used to verify if existing SMS messages on a Nokia 6021 handsets are able to be altered. The report shows that altering the sender’s number and message content for identifying falsified SMS messages were also possible, which can be pursued in the event suspicions are raised.

Index Terms - Cell Phone Forensics, Mobile Phone, SMS, Text messages.

I. Introduction

We have been asked on a number of occasions to comment on messages presented as evidence that could have been falsified. This leads to three questions on the examination of SMS messages: 1) has the software used in the examination produced an inaccurate report, 2) has the report been modified after it was created, and 3) is it possible to modify/falsify the SMS messages on the handset?

The first two questions can be both answered by performing an examination of the relevant evidence and a comparison between the report findings and the SMS messages stored on the phone, assuming that the integrity of the examination has been maintained.

THE SMS MURDER MYSTERY: the dark side of technology

Robert Burnett, Karlstad University, Sweden
Ylva Härd af Segerstad, Göteborg University, Sweden

The network society is characterised by electronic communications more than not in digital form. While these developments and their economic benefits, they also pose many social and ethical challenges. The developed and resulting services can cause significant consequences for society at large. It is therefore important that the rights of individuals are protected. To this end, the United Nations has adopted the Universal Declaration of Human Rights. "No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. Everyone has the right to respect for his or her honour and reputation. Everyone is entitled in full equality to the protection of the law against such interference or attacks."

To date, an international harmonization of data protection has not been achieved due to cultural, historical, and political factors. In the United States, for example, data protection laws are frequently considered a design criterion for information systems.

A Study on the Forensic Data Extraction Method for SMS, Photo and Mobile Image of Google Android and Windows Mobile Smart Phone

Woo-Sung Chun and Dea-Woo Park

Dept. of IT Application Technology, Hoseo Graduate School Of Venture, Korea
dexus8522@gmail.com, prof_pdw@naver.com

Abstract - Lately the use of Mobile Phone has been saturated and the use of Smartphone including iPhone had rapidly increased. At present there are 3 kinds of Forensic Data Extraction methods which are SYN, JTAG and Revolver. However, different Forensic Data Extraction methods should be used depending on the difference in Mobile Phone and Smartphone technology and how to use them. This thesis aims at studying on Forensic Data Extraction method in the case of Smartphone. For the analysis of Google Android and Windows Mobile Smart Phone which are mainly used for Smartphone, Spec. and O.S. analysis as well as Data analysis are conducted, and evidence data are created by extracting Forensic data of Google Android and Windows Mobile Smartphone. The research on the technology experimented through this research will contribute to the development of Mobile Phone Forensic technology.

Keywords: Smartphone, Mobile Forensic, Windows Mobile, Android.
GPS

Digital Trails Discovering of a GPS Embedded Smart Phone – Take Nokia N78 Running Symbian S60 Ver 3.2 for Example

Hai-Cheng Chu, Li-Wei Wu, Hsiang-Ming Yu, and Tzeng-Jong Lin

1 Department of International Business, National Taichung University of Education, 140 Min-Shen Road, Taichung, Taiwan
2 Department of International Business, Tunghai University, No.181, Sec. 3, Taichung Port Rd., Taichung, Taiwan
3 Department of Computer Science and Engineering, Seoul National University of Technology, 172 Gongneung-dong 2-ga, Nowon-gu, Seoul, Korea

gpschu@mail.ntcu.edu.tw, lwu@thu.edu.tw, bradpark91@hotmail.com

Abstract. As mobile computing devices become pervasive in daily lives, it is particularly critical for law enforcement agencies to be aware of their specific use. In the case of Global Positioning System (GPS), the embedded Global Positioning System device is used to disclose the locations of the objects that they wish to go via data mining technology. From digital forensic exploration of mobile phones, digital evidences essentially play a critical and decisive role in criminal, cybercriminal or cyber terrorism cases although the devices and the corresponding operating systems. The generic guides and methodologies for the law enforcement and digital forensics specialists to ponder when they deal with the evidences. The NIST GPS secure computing device is non-volatile memory; smart phone.

Expanding the Potential for GPS Evidence Acquisition

Chad Strawn

Abstract: This paper looks at the use of Global Positioning System (GPS) data for evidence collection and investigation purposes. The number of devices carrying GPS capabilities has increased over the years, investigators can find these to be helpful in deducing the elements of a crime, and criminals may attempt to thwart investigators by manipulating the data found on a GPS device in an effort to gain an advantage to support their activities. This paper discusses the Global Positioning System network, what type of devices and software is related to GPS, and the information that may be collected during an investigation involving GPS receivers.

Index Terms – GPS, forensics, navigation, multipathing, WAAS, AGPS, LBS, geotagging, waypoints, POIs.

1. INTRODUCTION

TECHNOLOGY has greatly changed the way criminals and investigators conduct business over the years. Criminals try to stay one step ahead of the law by adopting technology and using it as a means to conduct business quietly and quickly. Investigators are constantly pursuing offenders in an attempt to thwart their activities and it has turned into a game with both sides trying to learn the inner workings of new technology to work in their favor. In the past few years the market for Global Positioning Devices (GPS) has grown immensely and has become quite affordable to the average citizen. GPS units have diminished in size from the large chunky models first introduced to the public and now the technology is often a standard option on many other electronic devices as well as the locations of all other satellites in the system.

Understanding the algorithms and computations required to diagnose the location of a device, but one should be able to understand the principles and limitations of the design. The GPS system was developed by the United States Department of Defense as a tool for the military that could help soldiers navigate foreign territory and deliver munitions precisely on target. The satellite-based system was first employed in 1978 and now consists of a total of 24 satellites that continuously orbit the earth [1]. The system was strictly used for military operations initially, but the United States government opened up the service for civilian use in the 1980s. The signal supplied to the civilian sector suffered from Selective Availability (SA), which was an intentional degradation of the signal accuracy to make sure that adversaries of the country did not have the ability to mount attacks with the same precision as the United States. Selective Availability was turned off in 2000 by the United States and civilian receivers have gained a greater rate of accuracy since.

The satellite system is supported by a network of ground stations that monitor the data sent by the satellites and transmit corrective data back to the satellites [2]. As the satellites orbit the earth they send out two different radio signals designated L1 and L2. L1 is set aside for civilian use and transmits data that can be read by civilian receivers to determine location. These signals contain three pieces of information called ephemeris data, almanac data, and pseudorandom code. Ephemeris data contains the precise location of the satellite as well as the locations of all other satellites in the system.

GTFS
National Institute of Standards and Technology
U.S. Department of Commerce
Hashing Techniques for Mobile Device Forensics

Shira Danker  Rick Ayers  Richard P. Milsan

Abstract: Previous research conducted at the National Institute of Standards and Technology has shown that mobile device internal memory hash values are variable when performing back-to-back acquisitions. Hash values are beneficial in providing examiners with the ability to filter known data files, match data objects across platforms and prove that data integrity remains intact. The research conducted at Purdue University compared known hash values with reported values for data objects populated onto mobile devices using various data transmission methods. While the results for the majority of tests were uniform, the hash values reported for data objects transferred via Multimedia Messaging Service (MMS) were variable.

Index Terms - Cell Phone Forensics, Mobile Device Forensics, Hashing, MMS, MD5.

I. INTRODUCTION

With the increasing popularity and technological advances of mobile devices, new challenges arise for forensic examiners and toolmakers [2]. Data recovered from mobile devices has proven useful in solving incidents and investigating criminal activity [3]. Cryptographic hash functions provide forensic examiners with the ability to verify the integrity of acquired data. The resulting hash value, a fixed-size bit string, is often used to identify known files and illustrates that data has not been modified. The two most commonly used hash functions are MD5 and SHA-1 [4].

Minimal research has been performed on how mobile phone forensic tools report hash values for individual data objects. Recent research conducted at Purdue University explored the hash results reported by mobile device forensic tools for acquired graphical images (e.g., .jpg, .bmp, .gif). While research conducted shows consistent behavior across mobile forensic tools, the following area of concern illustrates the need for future research: data objects transferred using Multimedia Messaging Service (MMS).

II. TERMINOLOGY

Data Transfer Methods: Communication channels (e.g., Bluetooth, Multimedia Messaging Service, etc.) provide a conduit to populate the internal memory of mobile devices.

Secure Hash: A mathematical algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that any change to the data will modify the hash value.

Mobile Device Data Objects: Individual files (e.g., .jpg, .bmp, .gif, etc.) residing in the internal memory of the mobile device.

Mobile Device Forensic Tool: Acquisition tools designed to perform a logical acquisition from the internal memory of mobile devices.

Personal Computer Forensic Tool: Forensic tools designed to acquire data from hard drives (e.g., IDE, SATA, SCSI, etc.)

III. PREVIOUS RESEARCH

Previous research on mobile device forensic tool hash generation has been minimal. Ayers, Jansen, Moenner, and Delaite [5] performed a series of tests using multiple mobile forensic tools in an update to their previous publication regarding an overview of forensic software tools for mobile devices. Two tests related to hashing were conducted: one to determine if mobile forensic applications reported consistent overall case hash values when performing back-to-back acquisitions, and the other to validate the reported hash values of individual files (i.e., data objects) from subsequent acquisitions. While their research showed that the overall case
Forensic Data Recovery from Flash Memory

Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Klis

Abstract—Current forensic tools for examination of embedded systems like mobile phones and PDAs mostly perform data extraction on a logical level and do not consider the type of storage media during data analysis. This paper suggests a low level approach for the forensic examination of flash memories and describes three low-level data acquisition methods for making full memory copies of flash memory devices. Results are presented of a file system study in which USB memory sticks from 45 different make and models were used. For different mobile phones is shown how full memory copies of their flash memories can be made and which steps are needed to translate the extracted data into a format that can be understood by common forensic media analysis tools. Artifacts, caused by flash specific operations like block erasing and wear leveling, are discussed and directions are given for enhanced data recovery and analysis on data originating from flash memory.

Index Terms—embedded systems, flash memory, physical analysis, hex analysis, forensic, mobile phones, USB sticks.

I. INTRODUCTION

THE evolution in consumer electronics has caused an exponential growth in the amount of mobile digital data. The majority of mobile phones nowadays has a build in camera and is able to record, store, play and forward picture, audio, and video data. Some countries probably have more memory sticks than inhabitants. A lot of this data is related to human behavior and might become subject of a forensic investigation.

Flash memory is currently the most dominant non-volatile solid-state storage technology in consumer electronic products. An increasing number of embedded systems use high level file systems comparable to the file systems used on personal computers. Current forensic tools for examination of embedded systems like mobile phones or PDAs mostly perform logical data acquisition. With logical data acquisition it's often not possible to recover all data from a storage medium. Deleted data for example, but sometimes also data which is not directly relevant from a user standpoint, can not be acquired and potentially interesting information might be missed. For this reason data acquisition is wanted at the lowest layer where to file system level where tools can be used for forensic data originating from flash memory. Chapter V explains data originating from flash memory.

II. FPGA

Flash memory is a type of memory that is electrically erased and reprogrammed in two flavors, NOR! flash and NAND flash. NOR flash is the basic logic structure flash. NOR flash can be either symmetrical or non-symmetrical, which is the reason why it is used for system memory. The flash memory of the flash memory is required to be a part of the NOR flash that is used for user data storage. Disks, or multimedia, camera phones, USB flash memory sticks, mobile data storage, this technology first introduced in the perspective. An introduction found in [5], more in detail A. Physical Characteristics

The physical mechanism based on storing electric charge. This charge can be stored on a transistor. This charge can be applied to a memory cell and it will leak away caused specifications for current 100 years.

Flash memory can be erased but it has to be erased completely. Erasing result in " 1 "s. In NAND flash memory, the erase operation can be performed on a page basis. This means that all pages on a certain block will be erased simultaneously. In contrast, in NOR flash memory, each page must be erased individually. This can be a time-consuming process, especially for large flash memories. The erase operation can be performed on a sector basis. This means that all sectors on a certain block will be erased simultaneously. In contrast, in NOR flash memory, each sector must be erased individually. This can be a time-consuming process, especially for large flash memories. The erase operation can be performed on a block basis. This means that all blocks on a certain chip will be erased simultaneously. In contrast, in NOR flash memory, each block must be erased individually. This can be a time-consuming process, especially for large flash memories. The erase operation can be performed on a chip basis. This means that all chips on a certain host will be erased simultaneously. In contrast, in NOR flash memory, each chip must be erased individually. This can be a time-consuming process, especially for large flash memories.

III. Conclusion

The use of flash memory in mobile devices has increased significantly in recent years. This is due to the advantages of flash memory, such as low power consumption and high storage density. However, flash memory is also prone to data corruption due to various factors such as wear-out, bit flips, and charge injection. These factors can lead to data loss, which can be catastrophic in some cases. Therefore, it is important to have a reliable data recovery process that can recover data from flash memories in the event of data loss.

IV. Conclusion

This paper has presented a low level approach for the forensic examination of flash memories. The approach is based on the use of low-level data acquisition methods and the analysis of flash memory artifacts. The results of the file system study show that USB memory sticks from different makes and models can be fully recovered. This approach can be used to enhance the forensic investigation of mobile devices. Further research is needed to improve the approach and to develop more efficient data recovery methods.
The iPhone Meets the Fourth Amendment

Adam M. Gershowitz

Imagine that Dan Defendant is stopped by the police for driving through a stop sign. The officer thinks that Dan looks suspicious, but has no probable cause to believe he has done anything illegal, other than driving recklessly. Nevertheless, because running a stop sign is an arrestable offense and the officer is suspicious that Dan might be involved in more serious criminal activity, the officer arrests Dan for the traffic violation.

Under the search incident to arrest doctrine, officers are entitled to search the body of the person they are arresting to ensure that he does not have weapons or will not destroy any evidence. The search incident to an arrest is automatic and allows officers to open containers on the person, even if there is no probable cause to believe there is anything illegal inside of those containers. For instance, a standard search incident to arrest often turns up drugs located in a small container such as a cigarette pack. Yet, Dan does not have a cigarette pack in his pocket; instead, like millions of other technophiles, Dan is carrying an iPhone.

The officer removes the iPhone from Dan’s pocket and begins to rummage through Dan’s cell phone contacts, call history, emails, pictures, movies, and, perhaps most significantly, the browsing history from his use of the internet. In addition to finding Dan’s personal financial data and embarrassing personal information, the police also discover
CELLULAR PHONES, WARRANTLESS SEARCHES, AND THE NEW FRONTIER OF FOURTH AMENDMENT JURISPRUDENCE

MATTHEW E. ORSO

INTRODUCTION

Advances in technology and science have always presented challenges in applying constitutional search and seizure law. In this context, the Supreme Court has considered whether law enforcement may, absent a warrant, eavesdrop on private telephone conversations and use radio transmitters to track the public and private movements of suspects. The Court has addressed questions regarding whether the aerial surveillance of land and the use of a thermal imaging device to gather information about the inside of a home constitute searches under the Fourth Amendment. Further, it has tackled such issues as the legality of mandatory urinalysis for high school athletes and chemical testing in the field of suspected drugs that have been seized by law enforcement.

Yet as one court has appropriately observed, “The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.” A quick glance at the edge of this new frontier might reveal the following: the FBI’s “Magic Lantern” technology, a Trojan horse virus that remotely injects surveillance programs onto a suspect’s computer and records
Operating Systems
Android
Mobile Device Analysis
Shafik G. Punja & Richard P. Milsan

Abstract—The increased usage and proliferation of small scale digital devices, like cellular (mobile) phones has led to the emergence of mobile device analysis tools and techniques. This field of digital forensics has grown out of the mainstream practice of computer forensics. Practitioners are faced with various types of cellular phone generation technologies, proprietary embedded firmware systems, along with a staggering amount of unique cable connectors for different models of phones within the same manufacturer brand.

This purpose of this paper is to provide foundational concepts for the data forensic practitioner. It will outline the common cell phone technologies, their characteristics, and device handling procedures. Further data evidence storage areas are also explained along with data types found in the various storage areas. Specific information is also noted about BlackBerry and iPhone devices.

Detailed procedures for data analysis/extraction for mobile devices and how to use the various toolkits that are available is beyond the scope of this paper; the staggering numbers of cell phones and the intricacies of the toolkits makes this impossible. However, resources for the reader to further investigate the topic are attached in the appendix.

Index Terms—Mobile Device, Cell Phones, BlackBerry, PDA, Smart Phones, Cellular Phone Generation, CDMA, TDMA, GSM, iDen, SIM, IMEI, IMSI, ICCID, ESN, MEID, PIN, PUK, Flash Memory, Memory Cards, Mobile Device Analysis, Analysis Tools, Cell Phone Forensics

I. INTRODUCTION

The area of digital forensics (computer forensics), has grown rapidly in the 21st century, most notably due data/information/evidence, and the techniques and tools for properly handling mobile devices.

II. MOBILE DEVICES

Let us first clarify some terms in relation to mobile devices. For the sake of this article, the use of mobile devices is not referring to thumb drives, USB drives, memory sticks, portable flash drives, or portable externally encased hard drives. Mobile devices specifically refer to Cellular (or Mobile) Phones, Portable Digital/Data Assistants (PDA's), and Smart Phones. Bear in mind that some of the older model PDA's, such as the initial Palm and BlackBerry series devices do not have radio (cellular) capability and are simply used to store personal information (contacts, calendars, memos, to-do lists, etc.).

Mobile Devices Representation:
1) Cellular Phones
   a) Code Division Multiple Access (CDMA) - Typically handset only
   b) Global Systems Mobile (GSM) - Handset and SIM
   c) Integrated Digital Enhanced Network (iDEN) - Handset and SIM
2) Portable Digital/Data Assistants (PDA's)
   a) Palm Pilots (Palm OS),
   b) Pocket PC's (Windows CE, Windows Mobile),
   c) Blackberry's (RIM OS) that contain no radio (cellular) capability,
BlackBerry Forensics: An Agent Based Approach for Database Acquisition

Satheesh Kumar Sasidharan and K.L. Thomas

Resource Centre for Cyber Forensics (RCCF)
Centre for Development of Advanced Computing (CDAC)
Thiruvananthapuram
{satheeshks, thomaskl}@cdactvm.in

Abstract. Digital forensics is a field of prime concern, as the cyber crimes are becoming dominant in the modern world. Gadgets like mobile phones and smart phones are very commonplace in today’s society with powerful features. Criminals started using handheld devices for committing crimes as it is easy to handle and always portable. BlackBerry is a widely used smart phone because of its unique features. As the usage is very high, the evidentiary value of this device assumes greater importance in the litigation process. The very common methodology applied in BlackBerry forensics is the IPD file generation using BlackBerry Desktop Manager. The methodology explained in this paper uses a different approach. Here forensic image of the BlackBerry handheld is generated using a software agent, which is injected on the device before acquisition. The tool also analyzes the forensic image and shows phone contents in different file viewers.

Keywords: BlackBerry, cell phone forensics, smart phone, hashing.
Forensic Extractions of Data from the Nokia N900

Mark Lohrum
Purdue University Cyber Forensics
West Lafayette, Indiana
mlohrum@purdue.edu

Abstract. The Nokia N900 is a very powerful smartphone and offers great utility to users. As smartphones contain a wealth of information about the user, including information about the user’s contacts, communications, and activities, investigators must have at their disposal the best possible methods for extracting important data from smartphones. Unlike with other smartphones, knowledge of forensic acquisition from the N900 is extremely limited. Extractions of data from the N900 are categorized into limited triage extractions and full physical extractions. The imaging process of the phone has been explained as is necessary for a full investigation of the phone. The types of data as called for in a limited data extraction have been identified, and the locations of these files on the N900 were detailed. Also, a script was created which can be utilized for a limited data extraction from a Nokia N900.

Keywords: mobile forensics, smartphone forensics, Nokia N900, Maemo.

1 Introduction

The technology of communications by mobile devices has greatly advanced. Radio communications have evolved into car phones, cellular telephones, camera phones, and smartphones, the newest evolution of mobile devices. Smartphones have become ubiquitous, and there exists a great variety of manufacturers and models of these devices, along with various operating systems. The Nokia N900, running the Maemo
Symbian Smartphone Forensics: Linear Bitwise Data Acquisition and Fragmentation Analysis

Vrizlynn L. L. Thing and Tong-Wei Chua

Digital Forensics Lab
Cryptography & Security Department
Institute for Infocomm Research, Singapore
{vriz,twchua}@i2r.a-star.edu.sg

Abstract. In this paper, we propose a forensics evidentiary acquisition tool for the Symbian smartphones. We design and build the acquisition tool to support a low-level bit-by-bit acquisition of the phone’s internal flash memory, including the unallocated space. After acquiring the raw image of the phone’s memory, we conduct experiments and analysis to perform a detailed study of the fragmentation scenarios on the Symbian smartphone. The objective of this work is to create a complete evidentiary data acquisition tool for the Symbian smartphone, analyse.
Forensic acquisition and analysis of palm webOS on mobile devices

Eoghan Casey*, Adrien Cheval, Jong Yeon Lee, David Oxley, Yong Jun Song

The Johns Hopkins University Information Security Institute, 216 Maryland Hall, Baltimore, MD 21218, USA

ABSTRACT

The emergence of webOS on Palm devices has created new challenges and opportunities for digital investigators. With the purchase of Palm by Hewlett Packard, there are plans to use webOS on an increasing number and variety of computer systems. These devices can store substantial amounts of information relevant to an investigation, including digital photographs, videos, call logs, SMS/MMS messages, e-mail, remnants of Web browsing and much more. Although some files can be obtained from such devices with relative ease, the majority of information of forensic interest is stored in databases on a system partition that many mobile forensic tools do not acquire. This paper provides a methodology for acquiring and examining forensic duplicates of user and system partitions from a device running webOS. The primary sources of digital evidence on these devices are covered with illustrative examples. In addition, the recovery of deleted items from various areas on webOS devices is discussed.

1. Introduction

The newest operating system created by Palm, called webOS, presents challenges and opportunities for digital investigators. The operating system is Linux-based and uses Java, Ruby, and various Web technologies to provide functionality common to mobile devices. This system is currently included on mobile devices, tablet computers, and “web-aware” appliances.

The primary test device used for this work was webOS 1.4.1.1 on the Dual Band 3G CDMA “Palm Pre Plus” cell phone. This device did not have a SIM card or removable memory card. This device has built-in GPS, supports Wi-Fi 802.11 b/g, and has a 3 mega pixel camera with multiple audio/video formats.
Introduction to Windows Mobile Forensics

Eoghan Casey, a,b, Mikhail Baran, b, John Doyle, b

aDell, Salt CRM, Baltimore, MD 21201, USA
bJohn Hopkins University, Information Security Institute, Baltimore, MD 21218, USA

Keywords:
Windows Mobile Forensics
Windows CE Forensics
Mobile Device Forensics
Cell Phone Forensics
CIDR Database
Transaction Logs
PST/PST, Mobile Software
Mobile Forensics

Abstract
Windows mobile devices are becoming more widely used and can be a source of valuable evidence in a variety of investigations. These portable devices can contain a large number of applications and operating systems, which allows for a wide range of potential forensic scenarios. Although forensic analysts can apply their knowledge of operating systems to Windows Mobile devices, there are often different operating systems, such as Windows CE, that need to be analyzed.

This paper provides an overview of Windows Mobile Forensics, describing the processes of acquiring and analyzing data on Windows Mobile devices. The key features of the forensic software on these systems are described, including multimedia, email, Web browsing, and reporting features. This includes an illustrative case involving mobile software monitoring software.

1. Introduction

Windows Mobile devices present a substantial opportunity and challenge for forensic practitioners. These devices are essentially computers that people carry in their pockets, which contain substantial amounts of information that can be useful from a forensic perspective, including communications, multimedia, and location information. These devices can be used for criminal purposes, including espionage, fraud, and data theft. The personal nature of the information on these devices can provide digital investigators with valuable insights into the nature of crimes and the activities of victims. In addition, investigations involving commercial, corporate, and military concerns must be able to detect the presence of programs that can be used to monitor the activities of Windows Mobile devices. New acquisition methods have become available that give forensic practitioners access to more information on these devices, including deleted data.

1.1 Tools for Interpreting and Analyzing Data

Tools for interpreting and analyzing data on Windows Mobile devices are becoming more advanced. These tools are designed to help forensic analysts to locate useful information. The tools available for Windows Mobile devices are designed to provide forensic analysts with a variety of tools to extract information from these systems.

1.2 Key Features

Windows Mobile devices are equipped with a variety of features that can be useful for forensic analysis. These features include multimedia, email, and Web browsing, and reporting features.

This paper describes the key features of mobile software monitoring software and the challenges facing forensic practitioners.

Keywords: mobile, smartphone, forensics, Windows Phone 7.

Windows Phone 7 from a Digital Forensics’ Perspective

Thomas Schaefer, Hans Höfken, and Marko Schuba
FH Aachen, University of Applied Sciences, 52066 Aachen, Germany
sch.thomas@gmail.com, (hoefken, schuba)@fh-aachen.de

Abstract
Windows Phone 7 is a new smartphone operating system with the potential to become one of the major smartphone platforms in the near future. Phones based on Windows Phone 7 are only available since a few months, so digital forensics of the new system is still in its infancy. This paper is a first look at Windows Phone 7 from a forensics’ perspective. It explains the main characteristics of the platform, the problems that forensic investigators face, methods to circumvent those problems and a set of tools that can be used for data collection.

This paper covers various topics and explains the main characteristics of the platform, the problems that forensic investigators face, methods to circumvent those problems and a set of tools that can be used for data collection.

Keywords: mobile, smartphone, forensics, Windows Phone 7.
A Comparison between Windows Mobile and Symbian S60 Embedded Forensics

Antonio Savoldi†, Paolo Gubian†, and Isao Echizen‡
†Department of Electronics for Automation, University of Brescia, Via Branze 38, Brescia, Italy
‡National Institute of Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan
† {antonio.savoldi,paolo.gubian}@ing.unibs.it, ‡echizen@nii.ac.jp

Abstract

The pervasiveness of communication devices, such as modern state-of-the-art smartphones, poses new challenges from a forensic standpoint. The differences between hardware and software mobile architectures create difficulties in the determination of reliable and general purpose procedures, which can be easily applied onto a general group of such devices. Therefore, we would like to present a general overview on how to reliably collect digital evidence with regard to Symbian (from 9.1 version onwards) and Windows-based mobile systems, by illustrating differences, issues, and a possible common methodology for dealing with this new challenging and emerging forensic field.

1 Introduction

to the traditional desktop/laptop systems, in terms of multimedia capabilities. For instance, a modern smartphone, which integrates functionalities of a cellular phone plus the PIM (Personal Information Manager) part of a PDA (Personal Digital Assistant), might have up to 128 Mbytes of SDRAM, up to 16 Gbytes of internal flash memory, different wireless built-in capabilities, such as Wi-Fi (Wireless Fidelity), Bluetooth, Infrared (Infrared Device Application), GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), HSDPA (High Speed Downlink Packet Access), a built-in high resolution camera, and, in high-level devices, a built-in GPS (Global Position System) receiver.

Apart from the increasing rate of diffusion of such devices, we need to ponder about the misuse and abuse of these embedded systems, by increasing the awareness of how it is possible to extract all the digital content from the observable memory of such systems, that is the complete
A Comparison between Windows Mobile and Symbian S60 Embedded Forensics

Antonio Savoldi\textsuperscript{d}, Paolo Gubian\textsuperscript{1}, and Isao Echizen\textsuperscript{d}

\textsuperscript{1}Department of Electronics for Automation, University of Brescia, Via Branze 38, Brescia, Italy
\textsuperscript{d}National Institute of Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan
\{antonio.savoldi,paolo.gubian\}@ing.unibs.it, eechizen@ni.ac.jp

Abstract

The pervasiveness of communication devices, such as modern state-of-the-art smartphones, poses new challenges from a forensic standpoint. The differences between hardware and software mobile architectures create difficulties in the determination of reliable and general purpose procedures, which can be easily applied onto a general group of such devices. Therefore, we would like to present a general overview on how to reliably collect digital evidence with regard to Symbian (from 9.1 version onwards) and Windows-based mobile systems, by illustrating differences, issues, and a possible common methodology for dealing with this new challenging and emerging forensic field.

1 Introduction

to the traditional desktop/laptop systems, in terms of multimedia capabilities. For instance, a modern smartphone, which integrates functionalities of a cellular phone plus the PIM (Personal Information Manager) part of a PDA (Personal Digital Assistant), might have up to 128 Mbytes of SDRAM, up to 16 Gbytes of internal flash memory, different wireless built-in capabilities, such as Wi-Fi (Wireless Fidelity), Bluetooth, IrDa (Infrared Device Application), GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), HSDPA (High Speed Downlink Packet Access), a built-in high resolution camera, and, in high-level devices, a built-in GPS (Global Position System) receiver.

Apart from the increasing rate of diffusion of such devices, we need to ponder about the misuse and abuse of these embedded systems, by increasing the awareness of how it is possible to extract all the digital content from the observable memory of such systems, that is the complete
and a few others worth mentioning...

Not found in the Journals...
I have been processing a lot of iPhone’s lately, and would like to share with you how many of the iPhone Forensic/Analysis tools fit into my Cell Phone/GPS tool classification system that I came up with several years ago. For those of you not yet familiar with the levels, I’ll review them and then dive right into classifying the tools that are currently available. If you are interested, please contact me directly via email (sam@sambrothers.com) and I’ll be happy to share a copy of my latest presentation for the classification of all Cell Phone/GPS tools as this is merely a sub-set of my original system.

![iPhone Tool Classification Diagram]

@ 2007 Sam Brothers

Basically, the levels are a system by which any Cell Phone or GPS forensic/analysis tools can be categorized into. As you move up the pyramid (generally):

- Methods get more “forensically sound”
- Tools get more expensive
- Methods get more technical
- Longer Analysis times
- More training required
- More invasive

Levels of Forensics

[More information and resources available at NIST, National Institute of Standards and Technology, U.S. Department of Commerce]
Notice of Violation of IEEE Publication Principles
Mobile Phone Forensics: Challenges, Analysis and Tools Classification

Authors

Notice of Violation of IEEE Publication Principles

"Mobile Phone Forensics: Challenges, Analysis and Tools Classification"
by Amjad Zareen, Shamim Baig

After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE's Publication Principles.

This paper contains significant portions of original text from the paper cited below. The original text was copied without attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

Due to the nature of this violation, reasonable effort should be made to remove all past references to this paper, and future references should be made to the following article:

"Cell Phone and GPS Forensic Tool Classification System"
by Sam Brothers
CELLULAR PHONE EVIDENCE
DATA EXTRACTION AND DOCUMENTATION
DET. CINDY MURPHY

DEVELOPING PROCESS FOR THE EXAMINATION
OF CELLULAR PHONE EVIDENCE

Recently, digital forensic examiners have seen a remarkable increase in requests to examine data from cellular phones. The examination of cellular phones and the extraction of data from the same present challenges for forensic examiners:

- The numbers of phones examined over time using a variety of tools and techniques may make it difficult for an examiner to recall the examination of a particular cell phone.

- There is an immense variety of cellular phones on the market, encompassing a variety of proprietary operating systems and embedded file systems, applications, services, and peripherals.

- Cellular phones are designed to communicate with the phone network and other networks via Bluetooth, infrared, and wireless (Wi-Fi) networking. To best preserve the data on the phone, it is necessary to isolate the phone from surrounding networks, which may not always be possible.

- Cellular phones employ many internal, removable, and online data storage capabilities. In most cases, it is necessary to apply more than one tool in order to extract and document the desired data from the cellular phone and its storage media. In certain cases, the tools used to process cellular phones may report conflicting or erroneous information, thus, it is critical to verify the accuracy of data from cellular phones.

- While the amount of data stored by phones is still small when compared to the storage capacity of computers, the storage capacity of these devices continues to grow.

- The types of data cellular phones contain and the way they are being used are constantly evolving. With the popularity of smart phones, it is no longer sufficient to document only the phonebook, call history, text messages, photos, calendar entries, notes, and media storage. The data from an ever-increasing number of installed applications should be...
CHIP-OFF AND JTAG ANALYSIS FOR MOBILE DEVICE FORENSICS

IN THE FIELD of mobile device forensics, the practices of “chip-off” and JTAG analysis have become topics of growing interest among the community. As mobile devices continue to bring new challenges to the examiner, these two disciplines warrant close attention, as they both offer examiners avenues for deeper data access, the ability to bypass lock codes, and a way to recover data from damaged devices. In addition, today’s intentional tech continues to provide innovations at an exponential rate and offers examiners expanding phone support with increasing data-erasure abilities; the unobservable reality is that there is a seemingly infinite number of devices that continue to challenge examiners, creating the requirement for alternative means of data recovery.

Unfortunately, the goal for the mobile-device forensic examiner is to obtain a physical image of the memory chip from mobile devices. And while today such a physical memory chip cannot be accomplished without direct access to the memory chip, additional means for devices that are damaged or locked with an encryption scheme that is beyond today’s tools are bypassing lock codes, the chip-off and JTAG methods are among the alternative solutions for examiners looking to gain access to the memory.

In a perfect world, the commercial tools would do it all, and the examiner could process easily and comprehensively the mounting issues of mobile devices in their lab. Unfortunately, that reality is quite contrary to the evidence as is done live on the set of CSI: Miami—and as anyone who has spent any time trying to acquire data from mobile devices knows, the general mix remains you never know what you will be confronted with next, and just how much data can be obtained. Further, considering that commercial tools and are used in the same way the forensic examiner is known to be a tool that contemplates the usability of the data through the devices performed via controllers that make it impossible to acquire a complete image of the memory. Simply put, chip-off or JTAG techniques are by far the only way to obtain a complete image on some devices.

This article aims to introduce the chip-off and JTAG techniques for the mobile device examiner and provide the basics for those who are looking to learn more.

Introduction to chip-off and JTAG

The chip-off technique encompasses the practice of removing a memory chip, or any chip, from a circuit board and replacing it. The chip-offs are programmed with the “JTAG” method. The term “JTAG” is derived from Joint Test Action Group, which is the original and one of the most widely used standards for the purpose of providing a standard for various processors and electronic devices.

This method utilizes a physical chip-off technique that provides a direct connection to the memory chip, allowing the examiner to extract data from the device. Additionally, for devices that are damaged or locked with an encryption scheme that is beyond today’s tools, the chip-off method can be used to bypass lock codes, and the JTAG method can be used to access the memory chip. The memory chip provides the examiner with the ability to acquire raw data from the memory chip. For the mobile device examiner, these techniques offer another way to access and acquire raw data from the memory chip.

Prior to engaging in the practice of chip-off or JTAG techniques, it is imperative to have a basic understanding of the techniques. Specifically, the examiner must have a familiarity with mobile device technology, including the memory chip types, how they manage data internally, and how to identify a chip-off.

Chip-off and JTAG are used to perform two important tasks: to recover data from mobile devices that are locked or damaged, and to access data from devices that are not accessible through conventional methods. These techniques have been developed to address the challenges faced by examiners when working with mobile devices.

While not covered in this article, readers are strongly encouraged to learn more about JTAG and to understand the following concepts:

- NAND Memory (TSOP and BGA)
- NOR Memory
- Flash Translation Layer—Controller Chips
- NOR Flash—Embedded in eMMC

Similarities and Differences Between Chip-Off and JTAG

Initially, the major difference between chip-off and JTAG is that the chip-off technique is a more destructive method; once a memory chip is removed from a mobile device, it cannot be returned to the original location. In addition, the memory chip is removed from the mobile device, the device cannot be restored, and the mobile device must be repaired as a whole.

On the other hand, the JTAG technique is less destructive. Once a memory chip is removed from the mobile device, it can be returned to the original location. The device can be restored, and the mobile device does not need to be repaired as a whole.

Evidence Technology Magazine • May–June 2012
www.EvidenceInMagazine.com
Academic Journals and Conferences
Digital Forensic Research Workshop

http://www.dfrws.org/2014/cfp.shtml

National Institute of Standards and Technology
U.S. Department of Commerce
Digital Investigation

http://www.journals.elsevier.com/digital-investigation/
Android Anti-forensics: Modifying CyanogenMod

Karl-Johan Karlsson
University of Glasgow
creidelki@lyutor.liu.se

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

Abstract
Mobile devices implementing Android operating systems inherently create opportunities to present environments that are conducive to anti-forensic activities. Previous mobile forensic research focused on applications and data hiding anti-forensic solutions. In this work, a set of modifications were developed and implemented on a CyanogenMod community distribution of the Android operating system. The execution of these solutions successfully prevented data extractions, blocked the installation of forensic tools, created extraction delays and presented false data to industry accepted forensic analysis tools without impacting normal use of the device. The research contribution is an initial empirical analysis of the viability of operating system modifications in an anti-forensics context along with providing the foundation for future research.

1. Introduction
The increasing integration of mobile smartphones, in today’s digitally dependent, highly networked, communication based societies creates an environment that poses challenges for forensic analysts. The installation of third-party applications and the increasing reliance on cloud services for data storage and transfer present additional challenges. This paper presents an initial empirical analysis of the viability of modifying the Android operating system to create a hostile environment for forensic analysts. The research contribution is a novel approach to modifying the Android operating system to prevent data extractions and block the installation of forensic tools. The research also provides a foundation for future work in this area.

Due to this acceptance, forensic analysts rely heavily on the correct functioning of the phone’s software when performing analyses. Hence, altering functionality is a way of thwarting an analysis. Smartphones running operating systems such as Android and iOS are designed to allow the installation of third-party applications. This has allowed for the development of applications with anti-forensic functionality [7, 12, 27]. However, these
International Conference on Digital Forensics an Cyber Crime

http://d-forensics.org/2014/show/home
The Journal of Digital Forensics, Security and Law

http://www.adfsl.org/journal.htm
Small Scale Digital Device Forensics Journal

http://www.ssddfj.org
Welcome to MFW09
All Day Long!

How "Forensic" are your Mobile Device Tools?

Leveraging Cell Phone and Network Information: Part 1

How Big is Your Iceberg?

Viability of Using Hash Values in Mobile Phone Forensics

A.M. Break

GPS Forensics

iPhone Forensics: The Good, Bad and Ugly

Faraday, Freaks and Fun - why isolate a phone?

On-Scene Triage Forensics of Mobile Phones

Lunch

Reference Materials for Cell Phone Forensic Tool Testing

Cell Phone Analysis: Technology, Tools, and Processes

Phone Spy-Ware: What's Bugging You?

Pen-Link 8.1 Analytical Suite

P.M. Break

Leveraging Cell Phone and Network Information: Part 2

Android Forensics

A Forensics Tool for Windows Mobile Devices

Using Bootloaders to Dump the Internal Flash Memory of Mobile Phones

Panel Discussion: Standards and Certification

BlackBerry Messenger

- Blue smiley face = conversation has been read
- Yellow smiley face = conversation has not been read; when you read a message you will change the message flag to blue smiley face
- (checkmark) = message sent from the sending device and may sit with the tower and can reside for up to two weeks with the tower depending upon receiving device's ability to accept messages.
A Call to Arms
An Invitation for Research
Android Anti-forensics: Modifying CyanogenMod

Karl-Johan Karlsson
University of Glasgow
crdeiki@lysator.liu.se

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

Abstract

Mobile devices implementing Android operating systems inherently create opportunities to present environments that are conducive to anti-forensic activities. Previous mobile forensics research focused on applications and data hiding anti-forensics solutions. In this work, a set of modifications were developed and implemented on a CyanogenMod community distribution of the Android operating system. The execution of these solutions successfully prevented data extractions, blocked the installation of forensic tools, created extraction delays and presented false data to industry accepted forensic component analysis, an analyst would start by disassembling the phone and removing the surface mounted memory chips, which is a delicate and highly risky procedure. The memory chips can be read by standardized readers, but the interpretation of the data depends on the software running on the phone. A much easier method is to let the phone run, and access the data through the normal interfaces provided by the software. However, this presents a high risk of data being modified, both as a normal function of the phone and/or by specialized anti-forensic applications. The savings in time and effort gained by the utilization of normal interfaces are.
Third Party Application Forensics on Apple Mobile Devices

Alex Levinson
Rochester Institute of Technology
alex.levinson@mail.rit.edu

Bill Stackpole
Rochester Institute of Technology
bill.stackpole@rit.edu

Daryl Johnson
Rochester Institute of Technology
daryl.johnson@rit.edu

Abstract
Forensics on mobile devices is not new. Law enforcement and academia have been performing forensics on mobile devices for the past several years. Forensics on mobile third party applications is new. There have been third party applications on mobile devices before today, but none that provided the number of applications available in the iTunes app store. Mobile forensic software tools predominantly address "typical" mobile telephony data - contact information, SMS, and voicemail messages. These tools overlook analysis of information saved in third-party apps. Many third-party applications installed in Apple mobile devices leave forensically relevant artifacts available for inspection. This includes information about user accounts, timestamps, geolocational references, additional contact information, native files, and various media files. This information can be made readily available to law enforcement through simple and easy-to-use techniques.

control of the device provider to being defined by the user.

1.1. Apple Devices

With the introduction of the iPhone, Apple Computer has created a mobile handheld platform that allows users to install and configure a wide variety of applications via their "app store". The iPad device, introduced in April 2010, runs most iPhone apps in full functionality, as well as some that have been modified specifically for use with this larger format device. Users select applications of their choice and install them on the device. The application is downloaded to the device from Apple’s servers and installed. The application can now be launched by the user. The application can store data about the user that customizes the app for their use or stores information about how and when they interact with the app. Apps are typically backed up to the personal computer of the user whenever the device is synced as well.
Chapter 9

FORENSIC ANALYSIS OF PIRATED CHINESE SHANZHAII MOBILE PHONES

Junbin Fang, Zoe Jiang, Kam-Pui Chow, Siu-Ming Yiu, Lucas Hui, Gang Zhou, Mengfei He and Yanbin Tang

Abstract Mobile phone use – and mobile phone piracy – have increased dramatically during the last decade. Because of the profits that can be made, more than four hundred pirated brands of mobile phones are available in China. These pirated phones, referred to as “Shanzhai phones,” are often used by criminals because they are inexpensive and easy to obtain. However, the variety of pirated phones and the absence of documentation hinder the forensic analysis of these phones. This paper provides key details about the storage of the phonebook and call records in popular MediaTek Shanzhai mobile phones. This information can help investigators retrieve deleted call records and assist them in reconstructing the sequence of user activities.

Keywords: Chinese Shanzhai phones, forensic analysis, phonebook, deleted data

1. Introduction

The use of mobile phones around the world has increased dramatically. According to the ITU, the number of global mobile subscribers reached 5.3 billion in 2011. During the first quarter of 2011 alone, ven-
Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services

George Grispos
University of Glasgow
g.grispos.1@research.gla.ac.uk

William Bradley Gilsson
University of Glasgow
Brad.Gilsson@glasgow.ac.uk

Tim Storer
University of Glasgow
timothy.storer@glasgow.ac.uk

Abstract
Cloud storage services such as Dropbox, Box and SugarSync have been embraced by both individuals and organizations. This creates an environment that is potentially conducive to security breaches and malicious activities. The investigation of these cloud environments presents new challenges for the digital forensics community.

It is anticipated that smartphone devices will retain data from these storage services. Hence, this research presents a preliminary investigation into the residual artifacts created on an iOS and Android device that has accessed a cloud storage service. The contribution of this paper is twofold. First, it provides an initial assessment on the extent to which cloud storage data is stored on these client-side devices. This view acts as a proxy for data stored in the cloud. Secondly, it provides documentation on the artifacts that could be useful in a digital forensics investigation of cloud services.

1. Introduction
Global connectivity, mobile device market penetration and use of remote data storage services are all increasing. Cisco reports that mobile data traffic reached 597 petabytes per month in 2011, which was over eight times greater than the amount of Internet traffic in 2000 [1]. They also predict that global mobile data transmission will exceed ten exabytes per month by 2016, with over 100 million smartphone users transmitting more than 1 gigabyte of data per month [1].

Supporting these predictions, cloud storage providers have experienced tremendous growth in the past year. A press release from Dropbox reported that their customer base has surpassed 25 million users [2]. They also claim that over one billion files are saved every three days using its services [3]. Box reports that enterprise revenue tripled in 2011 with mobile device implementation increasing 140% monthly [4]. Box have also experienced substantial penetration into the retail, financial and healthcare enterprise markets [5].

According to articles by CIO [6], surveys by Advanced Micro Devices (AMD) [7] and IBM [8], there is an apparent consensus that cloud computing is increasingly integrating into the business environment. The business reasons for this migration range from ideas like focusing on growth, innovation and customer value to improved use of resources, increasing employee productivity and cutting costs [8].
Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics

Marwan Al-Zarouni
School of Computer and Information Science
Edith Cowan University
forensics@marwan.com

Abstract
The paper gives an overview of mobile phone flasher devices and their use for servicing mobile phones, their illegitimate uses and their use in mobile phone forensics. It discusses the different varieties of flasher devices and the differences between them. It also discusses the shortcomings of conventional mobile forensics software and highlights the need for the use of flasher devices in mobile forensics to compensate for the shortcomings. The paper then discusses the issues with the use of flasher devices in mobile forensics and precautions and considerations of their use. The paper goes further to suggest means of testing the flasher devices and suggest some tools that can be used to analyse raw data gathered from mobile phones that have been subjected to flasher devices.

Keywords
Mobile Forensics, Cell Phone Forensics, Flasher Box, Hex Dumping, UPS-3 Tornado.

INTRODUCTION
The need to address issues with mobile phone forensics is ever important. The number of mobile phone users nowadays surpasses 2.5 billion people across 218 countries and territories (Smith and Pringle 2007). Mobile phone abuse and problems caused by the use of camera devices within mobile phones are also increasing (Tarica 2007). Yet, conventional mobile phone forensic solutions do not seem to keep up with advances in mobile phone technologies. Furthermore, the development cost for supporting less popular mobile phones by such forensic solutions contributes to driving the prices of such forensic solutions higher (Espiner 2007). This is in addition to expensive updates and yearly subscriptions or service agreements that are sometimes needed to get support for the latest mobile phone devices.

New types of devices called "flasher boxes", also know as "flashe", are relatively cheap and are now becoming significant additions to mobile forensic investigators' arsenal of forensic tools. These devices are being used by forensic investigators in Europe and the United States of America to acquire forensic images directly from mobile phones (Breeuwsma et al. 2007, Purdue 2007).
Validating Tools for Cell Phone Forensics

Neil Bhadsavle and Ju An Wang
Southern Polytechnic State University
1100 South Marietta Parkway
Marietta, GA 30060
(01) 678-915-3718
{nbhadsav, jwang}@spsu.edu

Abstract

As mobile devices grow in popularity and ubiquity in everyday life, they are often involved in digital crimes and digital investigation as well. Cell phones, for instance, are becoming a media or tool in criminal cases and corporate investigation. Cellular phone forensics is therefore important for law enforcement and private investigators. Cell phone forensics aims at acquiring and analyzing data in the cellular phone, which is similar to computer forensics. However, the forensic tools for cell phones are quite different from those for personal computers. One of the challenges is in this area is the lack of a validation procedure for forensic tools, in order to determine their effectiveness. This paper presents our preliminary research in creating a baseline for testing forensic tools. This research was accomplished by populating test data onto a cell phone (either manually or with an Identity Module Programmer) and then various tools effectiveness will be determined by the percentage of that test data retrieved. This study will shed light and inspire on further research in this field. This research could be expanded further in several ways: First, while we were using a locked T-Mobile standard SIM card thus the amount of change that can be done is limited, a test SIM card or a Smart card which is unlocked will
The growing need for on-scene triage of mobile devices

Richard P. Mislan a,⁎, Eoghan Casey b, Gary C. Kessler c

a Purdue University, College of Technology, Department of Computer and Information Technology, Center for Education and Research in Assurance and Security, 401 N Grant Avenue, West Lafayette, IN 47907-2021, USA
b Johns Hopkins University Information Security Institute, USA
c Gary Kessler Associates, School of Computer and Information Science, Edith Cowan University, Australia

ABSTRACT

The increasing number of mobile devices being submitted to Digital Forensics (DFI) is creating a backlog that hinders investigations and can risk the safety and the criminal justice system. In a military context, the equipment from mobile devices can negatively impact troop and civilian safety. To address this problem, there is a need for more automated methods and tools to provide investigators with information in a timely period. This paper will evaluate the on-scene triage process, including handling and providing guidelines for standardization. The paper outlines basic requirements for automated triage, which may be performed by mobile forensics technicians rather than investigators. This paper formalizes the on-scene triage process, placing it firmly within the handling process and providing guidelines for standardization. In addition, this paper outlines basic requirements for automated triage.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


A quantitative approach to Triaging in Mobile Forensics

Fabio Marturana
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
marturana@libero.it

Gianluigi Me
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
me@di.uninor2.it

Rosamaria Berté
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
rosamaria.berte@libero.it

Simone Tacconi
Polizia di Stato e della Comunicazione
Rome, Italy
simone.tacconi@statero.it

I. INTRODUCTION

Cell phone, PDA, and new generation smartphone proliferation and use is on the increase all over the world. Worldwide sales of mobile devices to end users totaled 428.7 million units in the second quarter of 2011, a 16.5 percent increase from the second quarter of 2010, according to Gartner, Inc. (Fig. 1) [2].

Worldwide Mobile Device Sales to End Users by Vendor in 2Q 2011 (Thousands of Units)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>2Q 2011 (Units)</th>
<th>2Q 2010 (Units)</th>
<th>Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>19,128.8</td>
<td>8,763.0</td>
<td>4.6</td>
</tr>
<tr>
<td>LG</td>
<td>21,122.8</td>
<td>16.0</td>
<td>5.7</td>
</tr>
<tr>
<td>Sony</td>
<td>61,827.0</td>
<td>40.7</td>
<td>15.6</td>
</tr>
<tr>
<td>Nokia</td>
<td>97,366.9</td>
<td>22.0</td>
<td>29.9</td>
</tr>
</tbody>
</table>

The recent development of Mobile Forensics, a branch of Digital Forensics, is the answer to the demand for forensically sound examination.
Are We Relying Too Much on Forensics Tools?

Hui Liu, Shiva Azadegan, Wei Yu, Subrata Acharya, and Ali Sistani

Abstract. Cell phones are among the most common types of technologies present today and have become an integral part of our daily activities. The latest statistics indicate that currently there are over five billion mobile subscribers are in the world and increasingly cell phones are used in criminal activities and confiscated at the crime scenes. Data extracted from these phones are presented as evidence in the court, which has made digital forensics a critical part of law enforcement and legal systems in the world. A number of forensics tools have been developed aiming at extracting and acquiring the ever-increasing amount of data stored in the cell phones; however, one of the main challenges facing the forensics community is to determine the validity, reliability and effectiveness of these tools. To address this issue, we present the performance evaluation of several market-leading forensics tools in the following two ways: the first approach is based on a set of evaluation standards provided by National Institute of Standards and Technology (NIST), and the second approach is a simple and effective anti-forensics technique to measure the resilience of the tools.

Keywords: Cell phone forensics, Android, Smart phone, Cell phone forensics tool, Anti-forensics.
The Vendor Tools

Ad Hoc Reactive Methodology
a. User Has an Issue
b. Emails Problem to Vendor
c. Fixes Issue in Next Revision

Validation and Verification

How do we know what we don’t know!
Drinking the Kool-Aid

Research:
• Prove or disprove a hypothesis
• Learn new facts
• Advance the common body of knowledge

We have a need to know!
One more thing...

for Steve...
A critical review of 7 years of Mobile Device Forensics

Konstantia Barmatsalou a, Dimitrios Damopoulos a, Georgios Kambourakis a, Vasilios Katos b

a InforSecLab Laboratory of Information and Communications Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Samos GREECE, Greece
b Information Security and Incident Response Unit, Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Xantho, Xanthi, Greece

ARTICLE INFO

Article history:
Received 6 April 2013
Received in revised form 24 October 2013
Accepted 26 October 2013

Keywords:
Mobile Device Forensics
Smartphone
Security
Forensic acquisition
Mobile OS

ABSTRACT

Mobile Device Forensics (MDF) is an interdisciplinary field consisting of techniques applied to a wide range of computing devices, including smartphones and satellite navigation systems. Over the last few years, a significant amount of research has been conducted, concerning various mobile device platforms, data acquisition schemes, and information extraction methods. This work provides a comprehensive overview of the field, by presenting a detailed assessment of the actions and methodologies taken throughout the last seven years. A multilevel chronological categorization of the most significant studies is given in order to provide a quick but complete way of observing the trends within the field. This categorization chart also serves as an analytic progress report, with regards to the evolution of MDF. Moreover, since standardization efforts in this area are still in their infancy, this synopsis of research helps set the foundations for a common framework proposal. Furthermore, because technology related to mobile devices is evolving rapidly, disciplines in the MDF ecosystem experience frequent changes. The rigorous and critical review of the state-of-the-art in this paper will serve as a resource to support efficient and effective reference and adaptation.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

Internet and Information Technology (IT) are no longer a novelty, but a necessity in almost every aspect concerning people’s lives, extending to a great variety of purposes, infrastructures in minor and major criminal activities, led to the creation of a new discipline, namely Digital Forensics (DF), equivalent to classical forensics where “evidence analysis takes place using data extracted from any kind of digital electronic device” (Harrell and Mision, 2007).
MOBILES!
WHAT HAVE WE LEARNED?
WHERE ARE WE GOING?
DON'T WASTE YOUR MONEY

"PHABLETS" ARE COMING

COMBINE CELL PHONE AND TABLET
Research is sometimes difficult...
But, research is necessary!
Thank you!

www.mislan.com