A Cry for Help: Persuading Cell phone Developers to Get Involved with Digital Forensics

Kendra Carr[1]

Abstract – Computer Forensics predominantly concentrates on the accessibility of retrievable information from a particular device. This paper focuses on the recovery of information from cell phones and the admissibility of the recovered data in court. The rapid advancement of cell phones has enlarged the amount of activities a user can implement and the quantity of information held within the cell phone. Digital Forensic tools are used to help forensic investigators recover information and determine whether or not a crime was committed and to present the potential evidence in court. The growing awareness of the critical information discovered within cell phones has pressed for Digital Forensic tools to rapidly evolve. However, without the help of cell phone designers, forensic tool developers will continue to struggle to keep up with the constant growth of new cell phone releases. This paper states the importance of Digital Forensic tools for cell phones, describes available methods to retrieve information off a cell phone, and discusses the legal requirements for the presenting evidence in court. The goal of this paper is to identify the weaknesses in cell phone Digital Forensics and inform cell phone developers that the advancement of cell phone forensic tools will not occur rapidly without their help, involvement, and cooperation.

Keywords: Digital Forensics, Computer Forensics, cell phone

INTRODUCTION

In an era where cell phones are increasingly multiplying, the amount of data retrievable from a cell phone is quickly continuing to increase. This collection of data is very valuable to forensic investigators when trying to recover evidence for a particular crime. The growing awareness of the critical information discovered within cell phones has pressed for the rapid advancement of cell phone forensic tools. However, cell phone designers are constantly creating and updating new cell phone software faster than ever. New cell phone releases are frequently being issued out on the market. This constant development of new cell phone software is causing forensic developers to lag behind in creating tools that are sufficient in analyzing and removing data off a cell phone. Without the help of cell phone designers forensic tool developers will continue to struggle to keep up with the constant growth of new cell phone releases. This paper states the importance of Digital Forensic tools for cell phones, describes available methods to retrieve information, and discusses the legal requirements for presenting evidence in court. The goal of this paper is to identify the weaknesses in Digital Forensics of cell phones in order to inform cell phone developers that the advancement of cell phone forensic tools will not occur rapidly without their help, involvement, and cooperation.

Cell phones devices typically hold personal information such as contacts, text messages, email, pictures, calendars, and browser history. This list of data is the common type of information discovered on any typical cell phone. However, the volume of information found on a smartphone, such as Blackberry, Android, and iphone, increases with the addition of different applications (apps) that can be downloaded on the phone. Apps for banking, security control for your home, social networking, and maps that use global positioning system (GPS) locations are the popular apps used. The purpose of these apps and additional programs on a cell phone is to create an easy functional world for the users. Even though, the objective of permitting users to complete various tasks from any location appears harmless, these modest operations lead to the ease of committing more acts that are criminal.

[1] Department of Computer Science and Engineering, Mississippi State University, Box 9637, MSU, MS, 39762, klc340@msstate.edu

At the launch of the fame of cell phones, prior to smartphones and the accessibility to surf the web, a cell phone's core function was to place phone calls and send text messages. The only valuable information was the call history, which could be recovered from a phone company. For that reason, most digital crimes were committed computers. Since the overload of apps availability and improved functionality of cell phones, criminals have the opportunity of effortlessly committing crimes from their phones. Crimes such as cyber bullying, child pornography, fraud, and blackmailing are just a few. The more intricate apps that allow the user to turn off and on their home security system, or to unlock and lock their car doors present opportunities for malicious users to be more creative and devious their crimes. Cell phones with card readers that permit small businesses to complete card transactions from their phone just scream for the possibility for identity theft! Though these functional apps and programs are opportune and labeled as "cool", the main point is that they encompass a great deal of personal and sensitive data. This large amount of data in a cell phone can be stored in several locations within the device. These locations include the phone's embedded memory, the Subscriber Identity Module (SIM) card, and the phone's removable memory [2].

WHERE DATA IS STORED

Software and further data is accessible inside a cell phone's embedded memory. This area may be used to broaden the SIM memory, accumulate additional phone book data, call logs and so forth. The following are some examples of the additional information, which may be found in a phone's memory [2]:

- Phone settings
- Calendar information
- SMS/MMS messages
- Call log entries
- Time and date
- Ring tones
- Application executables

A considerable amount of embedded memory is available in present-day cell phones. Media data such as pictures, music, and videos are stored on removable memory such as an SD card. SIM card, used in Global Systems for Mobile Communications (GSM) phones, is a smart card which enables connection to GSM networks, and enables the subscriber to be uniquely identified in the network [2, 4]. The SIM card holds a number of files, which contain user's subscriber information, and personal information such as [2]:

- The International Mobile Subscriber Identity (IMSI), which is the SIM card's globally unique identifier
- Language preference and network (service provider) information
- Currency information, such as call charge counters
- Information about the current or most recent location of the cell phone
- Phone book contacts
- SMS messages (sent and received)
- Recently dialed numbers

DIGITAL FORENSICS

Digital forensics predominantly concentrates on the accessibility of retrievable information from a particular device. It involves the identification, preservation, extraction, documentation, and analysis of digital data. In Computer Forensics, investigators follow clear well-defined methodologies that can be adapted for specific situations. Such methodologies include the following three phases from [1]:

1. The Acquisition Phase saves the state of a digital system so that it can be analyzed later. Tools are used to copy (or make an image of) data from the suspect storage device to a trusted device.
2. The Analysis Phase takes the acquired data and examines it to identify pieces of evidence. This phase includes examining file and directory contents and recovering deleted content. This phase should use an

exact copy of the original, which can be verified by calculating an MD5 checksum. It is important that these tools show all data that exist in an image.

3. The Presentation Phase presents the conclusions and corresponding evidence from the investigation.

When approaching an investigation, because of a standard operating system (OS) and file structuring system, a computer forensic investigator has knowledge of the system before he or she begins the acquisition phase. In addition, this standard structure of directories and files within a computer system allows for the ease of the development of computer forensic tools. Tools such as FTK Imager and Encase permit easy retrieval and interpretation of potential evidence recovered from a computer. However, cell phone digital forensics requires an alternative approach. Similar to computer forensic tools, cell phone forensic tools are used to help investigators recover information from a cell phone and establish whether a crime has been committed. Assortments of forensic and non-forensic tools, accompanied by other accessories, are used by cell phone forensic analysts to attempt to retrieve data from cell phones [6]. Cell phone forensic techniques ought to follow the same well-defined steps of computer forensic; however, the "ability to extract that information in a manner that will not significantly change cell phone's memory is an obstacle to the development of such an application [6]."

WAYS TO EXTRACT DATA

One way to seize potential evidence from a cell phone is for the investigator to simply browse through the user interface of the actual device. Though a significant amount of data can be collected, certain data such as deleted text messages would not be accessible via this method [2]. This approach to recover information is highly impractical and problematic. The investigator could damage or modify the information on the cell phone.

The general way to extract data is from the phone's embedded memory using cell phone forensic software such as PhoneBase (Envisage System), Oxygen Phone Manger II, and Cell Seizure (Paraben) that are developed by a third party company. These applications claim to not modify any data on the cell phone and support a wide range of models. They are designed to have a similar look and feel of computer forensic applications such as FTK and Encase, which safely remove data [2].

When software applications like Paraben fail, the next step is to analyze the SIM card. To access the SIM card, a four-digit PIN-code (Personal Identification Number) is required. When the PIN-code fails or is forgotten, an eight-digit coded called PUK is needed. The PUK code is fixed and retained by the network provider, thus the investigator will be able to gain access to the PUK code. A smart-card reader can be used to access and read information from the SIM card. If the investigator wishes to access the SIM card logically, explicit software would be required to implement the GSM SIM access mechanism. SIM card contents are structured as a series of binary filled data files that can be manipulated by specific tools. These tools include SIM Manager Pro, SIMCON, and Cards4Labs. Cards4Labs is currently the most popular tool in the law enforcement community. Crafted at the Netherlands Forensic Institute, this software is unique in that it produces a text report on most of the content on the SIM card rather than storing a digital copy of the data on the computer [2, 4].

An additional method to extract data from a cell phone is the possible use of phone managers as discussed in [6]. Phone managers are normally offered directly from the manufacturer of the phone and kept up to date with maintenance for recently released cell phone models. "The software permits user data to be synchronized with a desktop computer and modifications to be made through the user interface." Phone managers potentially are tools that can automate data retrieval of common types of basic user data, such as phonebook entries and photos. Nevertheless, phone managers are not forensic tools and supplementary steps must be taken prevent data modification on the cell phone. Forensic tools used for cell phones avert the problem of modifying data on a phone by "confining the command options of the protocol used to communicate with the device to only those that are either known to be safe or involve very minor forensic issues." This method of filtering is a frequently used technique in computer forensics, generally implemented in hardware or software write-blockers. The authors of this paper present the implementation of a filter between the program manager application and the device being managed, which prevent risky protocol command from propagating throughout the device.

LIMITATIONS OF CELL PHONE FORENSICS TOOLS

When extracting potential evidence from cell phone devices, tools such as SIMCON, Paraben and manufactured phone managers can be beneficial. Though these techniques are widely used, they have their major limitations. With SIM cards, inadequate storage capacity forces most of the applicable data to be stored in embedded memory [5]. Therefore, not much valuable information can be recovered from it. Existing forensic software required to recover data from the embedded memory is not designed for every cell phone model. Paraben, a prominent provider of mobile phone forensic software, sell packages for examining only six cell phone manufacturer's phones [5]. Phone managers, though a great alternative, are only beneficial if a phone manager is available through the cell phone's manufacturer [6]. Furthermore, if a phone manager is available, there is a need to implement filters to keep from altering the data on the phone. The obvious solution to these limitations is to develop tools that are more efficient.

CONSTRAINTS OF CELL PHONE FORENSIC TOOLS

Forensic developers are having a hard time creating efficient updated tools because the "information in a cell phone's internal memory is structured not according to any particular standard [5]." Pertinent data like call histories are stored in proprietary formats in locations that change with each new cell phone release. Even the cable needed to access the phone's memory varies by model. Thus, constructing tools to extract data directly from the phone's memory is much more complex and costly. Without a standard structure for cell phone file formats it is impossible for cell phone forensic tools to constantly keep up with the new releases of cell phone models. Not having updated, efficient stable means to recover potential evidence from a cell phone raises concern about data accuracy when presented in the courtroom.

RULES OF THE COURT ROOM

"When a tool's output is introduced in a court trial, it must meet certain legal requirements [1]." To enter scientific evidence into a United States court a tool must be reliable and relevant. The trustworthiness of evidence generated from a digital forensics tool, is determined by the judge in a pre-trial Daubert Hearing. The Judge's responsibility in the Daubert Hearing is to determine whether the underlying methodology and technique used to identify the evidence was sound, and whether as a result, the evidence is reliable. The Daubert guidelines answer whether or not a procedure can be tested, the known error rate of the procedure, whether or not the procedure has been published and reviewed, and if the procedure is generally accepted in the relevant scientific community. The Daubert Test is an expansion of the Court's prior approach to the admissibility of scientific evidence. If the court feels as if the software or methods used to recover data from a cell phone are unreliable, then the valuable evidence is thrown out! Thus, it is extremely important to keep cell phone forensic tools and methods updated as well as establish trustworthiness. With the constant struggle to develop updated techniques, forensic tools are soon going to be seen as an unreliable source.

A CRY FOR HELP (CONCLUSION)

In an attempt to persuade cell phone developers to engage in the development of cell phone forensic tools, I have identified several limitations of cell phone digital forensics. In summary, the constant releases of new cell phone models hinder the development of cell phone forensics tools, which hinders the admissibility of the recovered data in court. One way to stop this domino effect is with the aid of cell phone developers and manufacturers. This is a plea to them to consider the jobs of forensic investigators and developers. Cell phone developers can help by constructing new ways to standardize file structures in the embedded memory of cell phones, allowing SIM cards to enclose more memory, and working along the side of forensic developers in creating new recovery tools. With the amplified amount of activities a user can implement criminal acts from a cell phone are going to continue to increase. As a cell phone user, developer, or forensic analyst, we all share a common goal of wanting to keep the bad guys from harming the innocent. Without the support, involvement, and cooperation from cell phone developers, forensic software tools will continue to lag in their evolution. Steve Jobs quoted that "[...] right now is one of those moments when we are influencing the future [3]." The time is now for cell phone developers to take a stand and get involved, for the development of cell phone forensics depends on it.

References

[1] B. Carrier, “Open Source Digital Forensics Tools: The Legal Argument,” @Stack, Oct. 2002.

[2] P. McCarthy, “Forensics Analysis of Mobile Phones”, BS CIS Thesis, University of South Australia, School of Computer and Information Science, Mawson Lakes, October 2005,http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf.

[3] S. Jobs, Brainy Quote, http://www.brainyquote.com/quotes/authors/s/steve_jobs_2.html#ixzz1ddBMdVD2.

[4] S. Willassen, *“Forensics and the GSM Mobile Telephone System,”* International Journal of Digital Evidence, vol. 2, issue 1, spring 2003.

[5] T. Moore, *“The Economics of Digital Forensics,”* Fifth Workshop on the Economics of Information Security, June 2006.

[6] W. Jansen, A. Delaitre, L. Moenner*, “Overcoming Impediments to Cell Phone Forensics,”* Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, IEEE, Jan 2008.

Kendra Carr

Ms. Kendra Carr received her Bachelor’s degree in computer science from Mississippi State University (MSU) in 2010. She is currently pursuing a Master’s degree in computer science from MSU; her expected graduation date is May 2012.