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 vulnerable in security and privacy. Cell phones, for instance, have been a target of spam and harassment. Sometimes, they become a media or tool in criminal cases or in 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 in this area is the lack of a validation procedure for forensic tools 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 lay a foundation for 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 provide for a greater range of area for data to be written. Second, a SIM card writer or an identity module programmer for direct writing onto a SIM card would also allow for population for a greater range of element files. Third, open source SIM card writers or identity module programmers and SIM card readers would be more ideal for reading/obtaining data and writing data so researchers have the ability to look at as well as modify code.

Keywords: Cell phones, Forensics, Security, Privacy.

1. INTRODUCTION

Cell phone usage has been soaring for the past ten years. According to the US federal government statistics, in the last half of 2007, 16% of US homes only used cell phones for calls and 13% had landlines in addition to cell phones but used their cells all of the time or nearly all of the time. Approximately 33% of people under age 30 have only cell phones. As cell phone use becomes more widespread, cell phone forensics becomes more and more important as cell phones are often found in crime scenes.

Forensics is used in all types of situations from internally in a corporate auditing case to a criminal investigation case commonly seen in the law enforcement world. Many crimes and other misconducts make forensics very important as a means of making the world a better place. Digital forensics is becoming important because our society is becoming more dependent of various computers and telecommunication tools and technologies. Cell phone forensics, being part of digital forensics, aims at the retrieval or gathering of data and evidence from mobile phones and similar devices used in daily life. Cell phone forensics allows investigators to answer questions of interest on a certain subject related to cell pone based communication. It is based on proven scientific methodology and norms to collect facts regarding an object, an event, or an artifact in certain time period to determine whether the object was in fact what it claimed to be or was alleged as being. In this effort of forensics, cell phone forensic specialists have encountered major challenges that hinder their work. As we know, mobile devices are becoming the main mobile computing power with all its constant upgrades, changed, and new additions, this has caused the

forensic specialists to undergo a lack in available forensic tools for retrieval that is compatible with today's uprising of newer model devices.

The main difference between cell phone forensics and computer forensics is that in cell phone forensics, one has to deal with multiple different hardware and software standards, which makes creating a universal standard tool near to impossible. Since the software is embedded and more special purpose than computers, solutions for obtaining data are not standardized thus causing a need for vast solutions. With the advent of new phones coming into the market at an exponential rate, as well as new companies coming into the market using a whole different blend of proprietary software, the problem has been even more compounded as time progresses. The purpose of a cell phone forensic tool is to obtain data from a cell phone without modifying the data. The tool should provide critical updates in time to keep pace of the rapid changes of cell phone hardware and software. The tools can be either forensic or non-forensic, which each of them providing different challenges as well as allowing for different solutions. Forensic tools are tools that are designed primarily for uncovering data from cell phones, while non-forensic tools are not designed for uncovering data but can be manipulated for that purpose. Two different methodologies have been used to address this situation, either reduce the latency period between the introduction of the phone and the time the cell phone forensic software is available for that phone or create a baseline to determine the effectiveness of a tool on a certain device.

The first method is to reduce the latency period between the time a cell phone gets on the market and the availability of the forensic tools and this is primarily done by adding a new layer called a phone manager protocol filtering, which is located at a higher abstraction level between the programming interface and the library, thus in a way achieving certain program data independence. The value of this method is increased by the fact that most phone managers use the Windows operating system. The main approach for this method is to obtain a phone manager and modify it so dangerous "write" commands cannot be issued, i.e. forensic scientists will not accidentally write data onto a phone under investigation and thus compromise or jeopardize a case. This modification to the phone manager is done by a program called filter. This filter will not only block dangerous write commands, but also will intercept data from the target phone in binary form and then send it to the phone manager for further decoding.

The second method is to provide a baseline or test data to evaluate forensic tools. With this method, the user populates the phone with certain data and then attempts to retrieve it with a forensic tool. Thus the baseline is the original data that is populated on the telephone. The baseline is usually set up by Identity Module Programming (IMP). The data that is obtained by the forensic tool from the cell phone is tested against the baseline and therefore one can determine what the effectiveness of the cell phone forensic tool is. The major identity module that is used today is called the Subscriber Identity Module or SIM card which is used to separate the personal information from the actual mobile device as well as hold onto phone numbers, names and network settings and allows for the portability between phones. The SIM card is broken up into a file system organization with root directory file subdivided into multiple directory files (DF) that contain the elementary files (EF) which holds the binary data. Thus creates another problem as the data that needs to be obtained could be contained anywhere in the elementary files. In order to insert the test data onto the SIM card an IMP (Identity Module Programmer) needs to be inserted and then it will be allowed to write test EF.

2. RESEARCH APPROACHES

A cell phone has a SIM (Subscriber Identity Module) card containing essential information about the subscriber. It stores the authentication program and personal information as well, such as phone book entries and text messages. The SIM card is obviously very important for cell phone forensics. Like a smart card, a SIM card typically contains a processor and 16-128 KB EEPROM (persistent electronically erasable, programmable read only memory). It also includes RAM for program execution and ROM for the operating system and applications. The cell phone operating system controls access to elements of the file system that is illustrated in Figure 1 below:

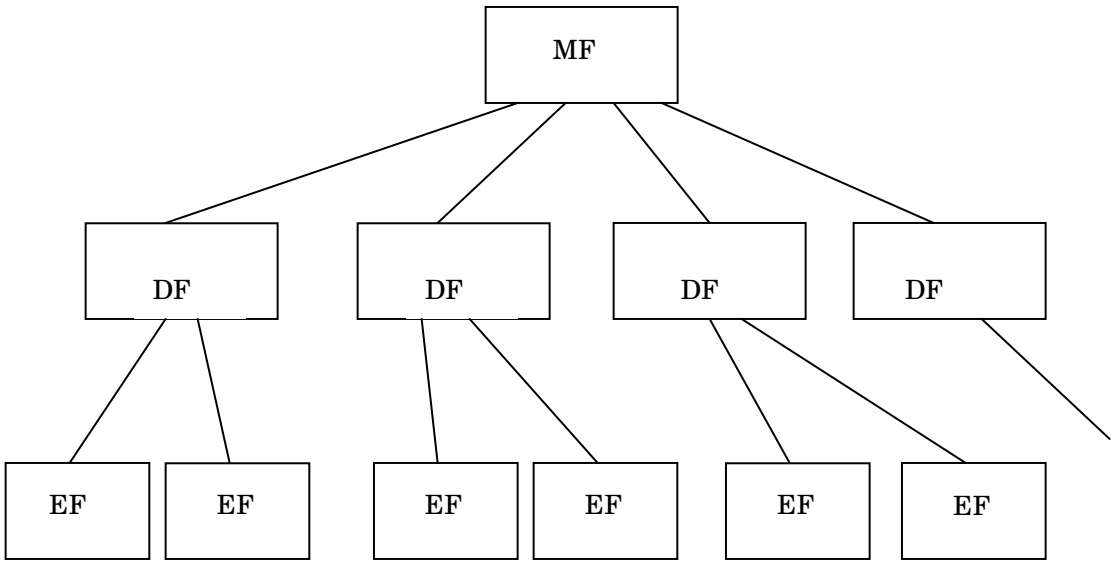

Figure 1 SIM file system

As shown in Figure 1, the SIM file structure consists of the root directory (MF), directory files (DF), and elementary files (EF). The valuable data for forensics located in the EFs. Data is generally populated with an Identity Module Programmer.

The approach for the project was to follow the second method mentioned previously. We first populated test data onto a SIM card and then retrieved the test data and determine the percentage of success rate for different forensic tools. The first step is to obtain a tool that supports SIM card reading and in this case Paraben [4] forensic tools was used as it supports protocols for reading SIM card data. The next step was the implementation of an Identity Module Programmer which was used to populate the EF's with test data, using an open source program called SIMBrush. This tool was used as it contains protocols for writing data onto a SIM card as well as reading data from the SIM card or programs similar to it. Once the test data is written onto the SIM card, Paraben Device Seizure was used to retrieve the data and determine the effectiveness by the amount of new data retrieved divided by the total data written onto the SIM card.

Our research involved the following materials:

- Motorola V3 Razr
- SIM card reader
- Paraben Device Seizure Toolkit(contained connecting wires) w/ CD
- MobTime Cell Phone Manager (trial version OK)

3. THE MAIN RESEARCH RESULT

The experiments were conducted on a cell phone, Motorola V3 Razr with a standard T-Mobile SIM card since the drivers were already installed for this phone and were available. Due to the unavailability of an identity module programmer, a cell phone manager was used to populate data onto the SIM card. The cell phone manager that was chosen to be used is called MobTime Cell Phone Manager by MobTime Inc. [5]. This program is a shareware program and thus we used the 30 day

free trail option, which allowed for basic reading and writing onto the phone as well as the SIM card. Initially the SIM card was read using the SIM card reader and the file structure was obtained, Device Seizure showed the basic file structure (the directory files (74FB, DCS1800, GSM, Telecom) with the individual EF's files in each of the directory files which show all the information that was stored) as shown in Figure 1. Once this is accomplished, the SIM card is reinserted into the phone and the phone is connected to the PC and MobTime is launched to start populating new test data. With MobTime the new data is added by adding new contacts to the address book (in the EF is called ADN located in the Telecom DF) and send new text messages back to the phone itself under experiment (SMS in the EF). Once this task was completed, the SIM card was removed from the phone and placed into the reader and the file structure was brought up again and the ADN was brought up and seen if this contact was now listed in this EF. The SMS could not be read since the data was encrypted in an unreadable format and thus the SMS was retrieved using the SMS History option in the data acquisition to retrieve the text messages in a readable form. The results were compared with the test data put in and the percent yield was determined. In this case with Phonebook and SMS data, the percent yield was 100%, as all the data put in previously was obtained.

Figure 2 illustrates the file structure of the T-Mobile SIM Card on Device Seizure showing the Directory Files:

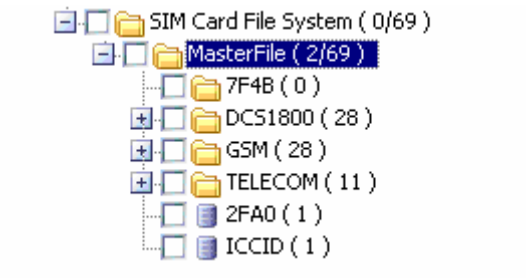

Figure 2 The file structure

There are two challenges in the field of cell phone forensics: One is that forensic tools fall far behind the great variety of new phone models and new phone products. Another is that many vendors claim that their forensic tools are more powerful, while users do not have a low-cost, effective way to validate these tools. For the first issue, our previous research has tested the solution of using cell pone managers as forensic tools. This requires extra work beyond just applying a phone manager provided by a new phone vendor. For instance, how to disable the "write" functionality of a cell phone manager could be a challenging task. For the second issue, this paper provides a low-cost approach to validate different forensic tools for cell phones. The research is very preliminary, but it lays a foundation for students in this area to test different forensic tools. The following five window captures demonstrate the intermediate results of the forensic process: Figure 4-6 show the population process using MobTime software tool. Figure 3 and 7 show the retrieved data using Device Seizure.

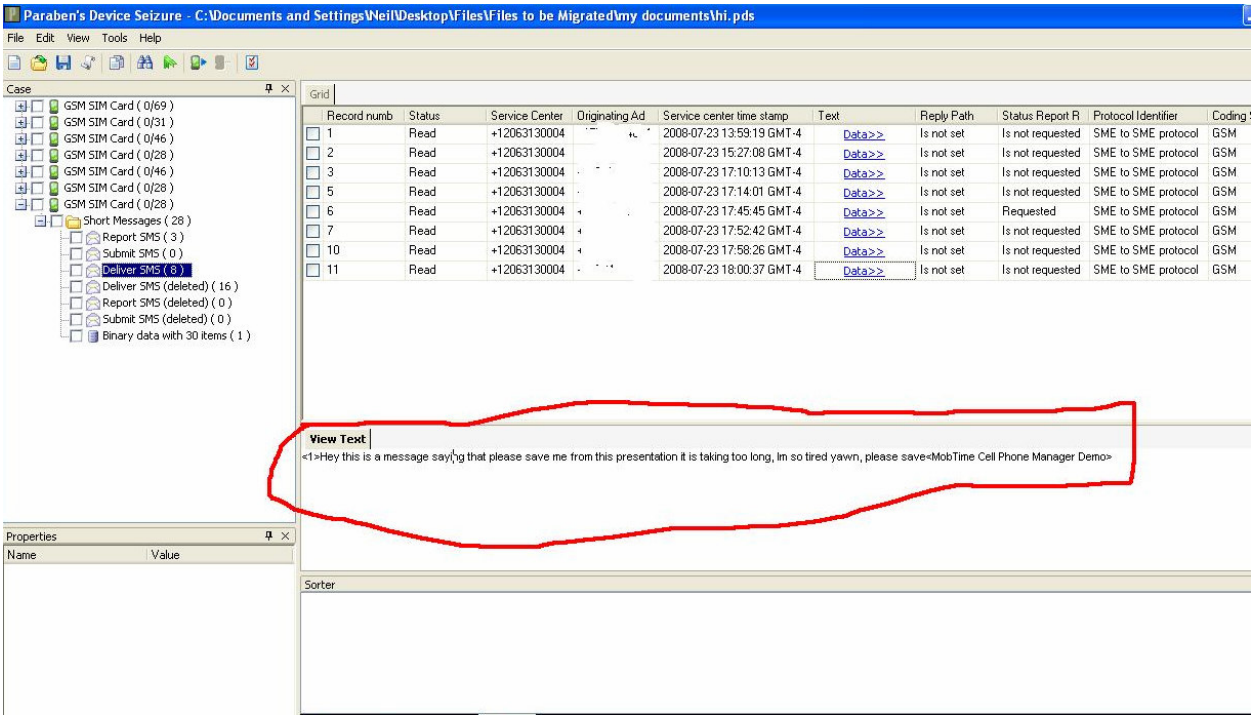

Figure 3 The retrieved data by Device Seizure

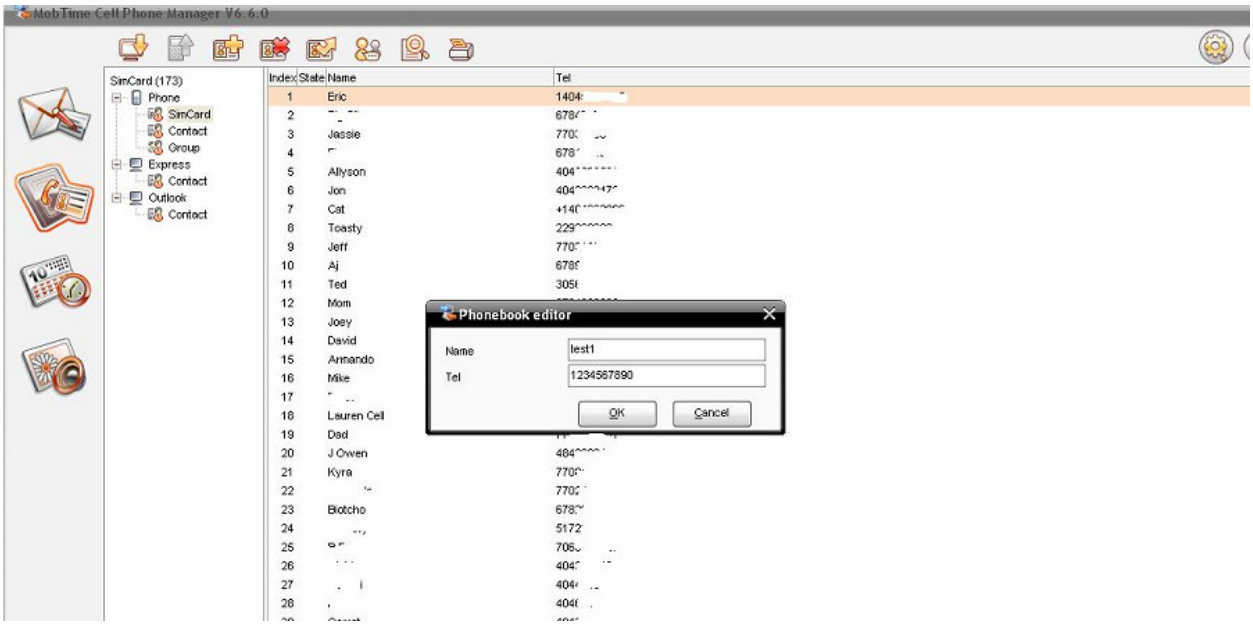

Figure 4 The populated data using MobTime

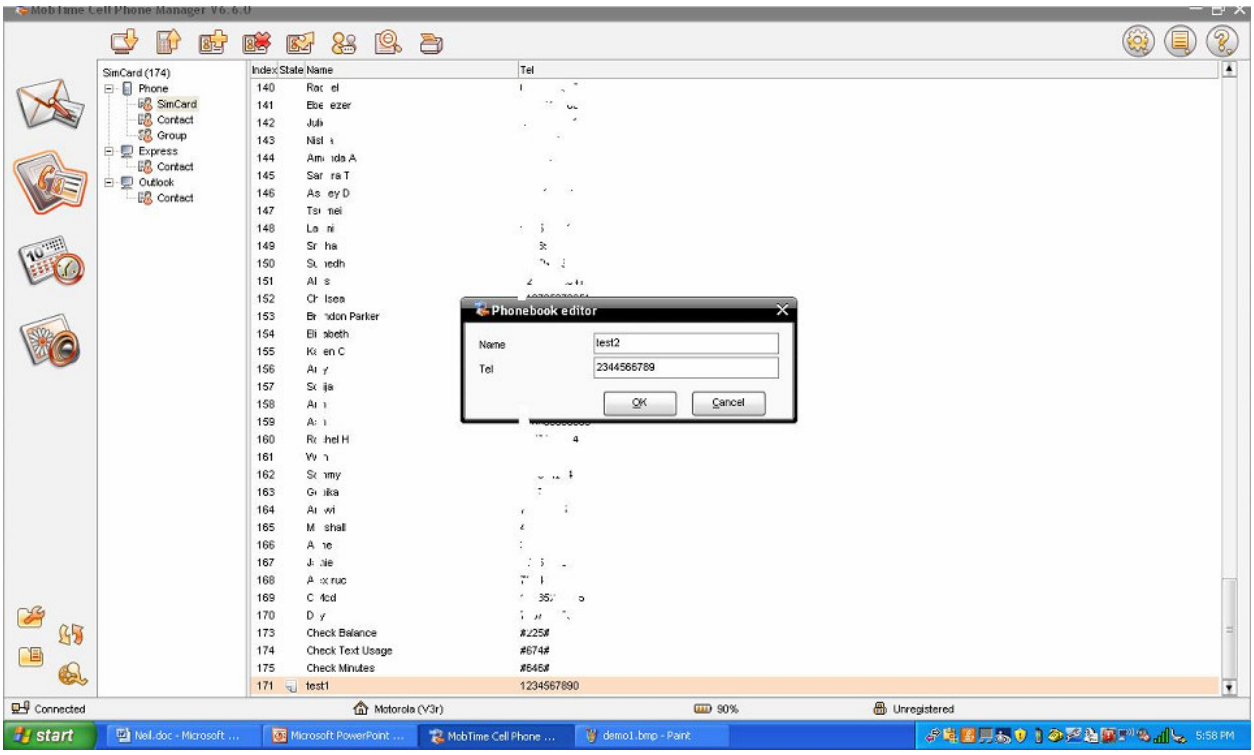

Figure 5 Another test with MobTime

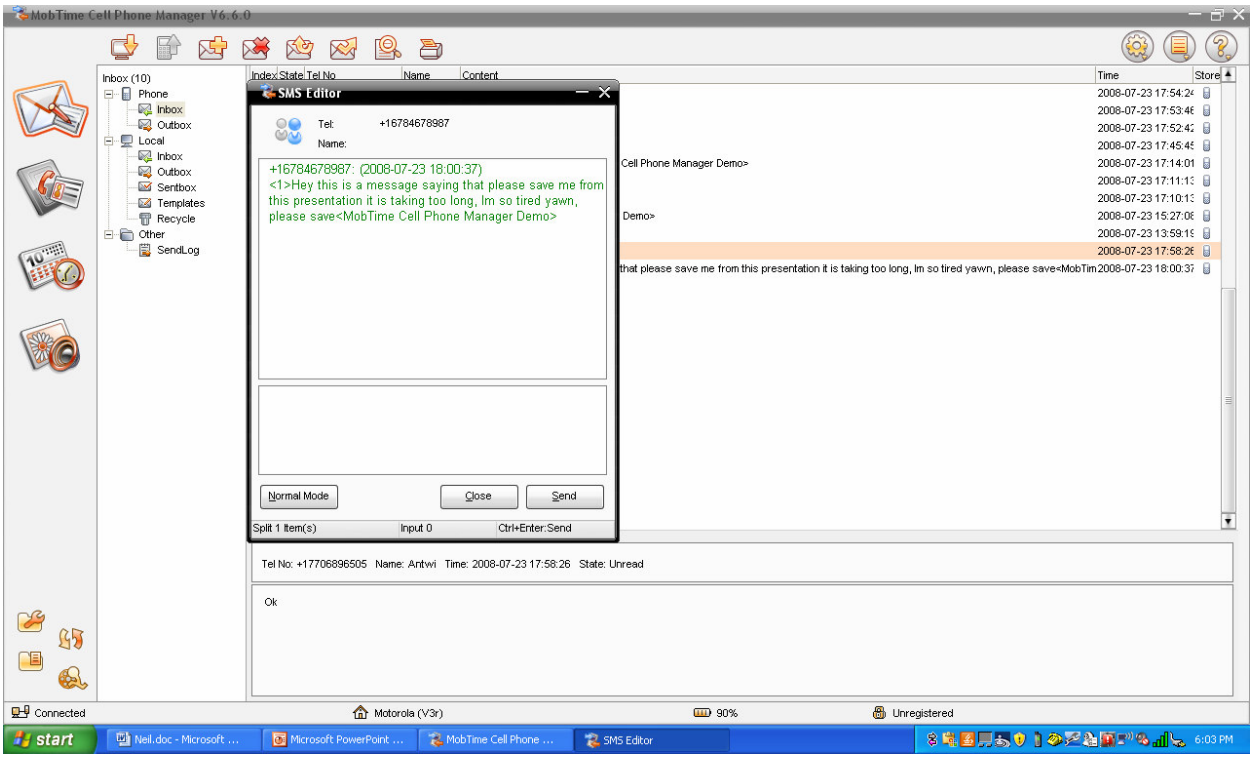

Figure 6 Data populated using MobTime

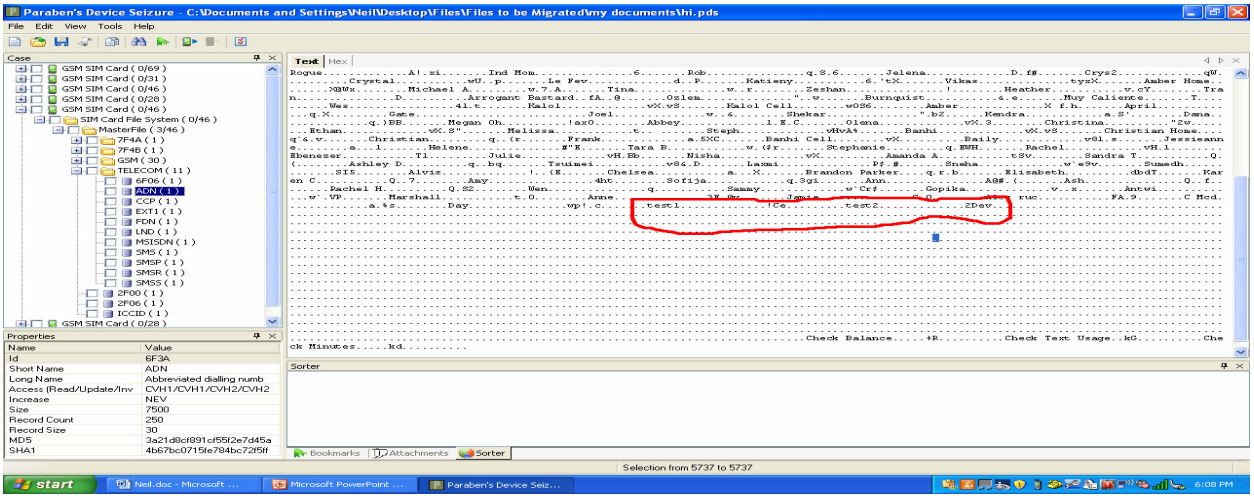

Figure 7 The retrieved data using Device Seizure

4. FURTHER RESEARCH TOPICS

This research was limited with the scope of time and equipment available. However, it provides a simple way to validate forensic tools for cell phones. This research could be expanded further by testing multiple cell phone forensic tools with the same baseline data. Since the SIM card used in our experiment was a T-Mobile standard SIM card which was locked, the amount of changes and modifications were limited due to the protection of the vital data or erroneously overwrite that data . It would be more interesting if we could test a SIM card or a Smart card which was unlocked, thus it would provide for a greater range of area for data to be written. Also a SIM card writer or an identity module programmer for directly writing onto a SIM card would also allow for population for a greater range of EF's to be populated. Moreover, open source SIM card writers or identity module programmers and SIM card readers would be more ideal for reading/obtaining data and writing data so researchers have the ability to look at them as well as modify them.

REFERENCES

[1] Jansen et. Al., Overcoming Impediments to Cell Phone Forensics.
[2] Jansen W. and Delaitre A., Reference Material for Assessing Forensic SIM Tools.
[3] Jansen W. and Ayers R., Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, May 2007.
[4] Paraben Corporation, Device Seizure 2.0, www.paraben.com.
[5] MobTime, MobTime Cell Phone Manager, http://www.mobtime.com/en/.

Note: T-Mobile is copyrighted by T-Mobile inc, Mob Time Cell Phone Manager is copyrighted by MobTime inc, and Device Seizure is copyrighted by Paraben corporation and are not endorsed by the researchers, only used for research purpose only.