2006

Forensic Analysis of the Contents of Nokia Mobile Phones

B. Williamson
Edith Cowan University

P. Apeldoorn
Edith Cowan University

B. Cheam
Edith Cowan University

M. McDonald
Edith Cowan University

Originally published in the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Forensic Analysis of the Contents of Nokia Mobile Phones

Williamson, B
Apeldoorn, P
Cheam, B
McDonald, M

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
bwillia3@student.ecu.edu.au

ABSTRACT

Acquiring information from a mobile phone is now an important issue in many criminal investigations. Mobile phones can contain large amounts of information which can be of use in an investigation. These include typical mobile device data including SMS, phone records and calendar and diary entries. As the difference between a PDA and a mobile phone is now blurred, the data that can reside on a mobile phone is somewhat endless. This report focuses on the performance of different mobile phone forensic software devices, and reports the findings. All aspects of the different software pieces will be reported, as well as what the investigators extract from the phones. The ability of different software tools to produce certain hash algorithm sums will be analysed, as well as the forensic methods used to extract the information. This area is one which will gain momentum in the future, hence any advances made in the field is an advantage to upcoming studies.

Keywords
Forensic, Mobile Phone, Nokia, Software, Analysis

INTRODUCTION

Mobile phones are an integral part of communication around the world today. Forensic and digital analysis of mobile phones is a relatively new area of interest, as crimes involving mobile devices are becoming increasingly common in the community. This has been compounded by the ability of modern mobile to store vast amounts of information, which has made them a very attractive target for law enforcement agencies. It is for this reason that forensic analysis of mobile phones is gathering momentum all over the world.

Mobile devices can contain a large amount of information covering a vast array of technologies. There are two main areas that can be analysed; phone data and data found on the Subscriber Identification Card (SIM). This study is focusing on the forensic analysis of the contents of mobile phone handsets. From this there are many smaller areas that can be broken down and analysed such as SMS history, call history and other memory stored. The aim of separating the study was to differentiate between the data found on SIM cards and the data found on the handsets analysed.

This report will cover what the expectations of the forensic analysis are and the methods used, as well as the hardware and software of the mobile handsets utilised. A summary of the final results will be included but will not include specific items recovered for privacy purposes. Any issues arising with either devices or software/hardware will also be noted.

BACKGROUND

A wide range of mobile phones and SIM cards were submitted to the University for testing, however only seven handsets were selected for analysis. The handsets collected were designed for use on GSM and CDMA networks. The idea was to collect many different mobile phones and SIM cards, and then forensically analyse them, to determine what data could be retrieved.

All of the handsets received were profiled, to determine the capabilities and features of each handset and give a basic idea of what information could potentially be retrieved from each device. This involved researching all of the different models of phones and then putting all of the information found into a spread sheet. This made it easier to understand what handsets could perform what particular tasks. For example, some handsets have Infrared and Bluetooth capabilities, where others are restricted to data cable only interactions with other devices. This was important because from this the investigators could be determined whether communication could occur wirelessly via Bluetooth or Infrared between the handsets. Similarly it also gave an idea of whether certain data could be realistically expected to be recovered from each type of handset. For example, some models of phones do not have memory that will store SMS so they could not be expected to return SMS messages when analysed.

As outlined, information can be stored on a mobile handset's internal memory, as well as the SIM card. Internal memory can be used to extend the SIM memory, and to store additional information, such as phone book entries and call logs (McCarthy 2005). Modern phones can hold a somewhat large amount of internal memory. The Nokia N91 has 4GB of internal memory, and this can also be extended via the use of an external memory card (Ciao GmbH 2006). These latest handsets often have a much larger amount of internal memory, as this is due to the ability to store more information onto a much smaller memory storage area. Also, a market push toward PDA type multi-purpose phones as opposed to phones purely designed for sending and receiving voice calls, which was the original, primary goal of the humble mobile phone.

The memory capabilities of a mobile phone can also be enhanced by the use of a compatible, removable memory card. These serve a similar purpose to those used for digital cameras, as they allow large files to be accessed instantly and expand the storage of the device. This is outside the scope of this report hence will not be covered any further.

Before discussing the findings it is appropriate to look at the potential information that can be extracted from mobile handsets. The internal memory of a mobile phone can store many different types of information. These can include, but are not limited to:

- Short Dial Numbers
1- Text Messages
2- Settings (language, date/time, tone/volume etc)
3- Stored Audio Recordings
4- Stored Computer Files, i.e. pictures and graphics
5- Logged incoming calls and dialled numbers
6- Calendar and possible Events
- Bookmarks
7- GPRS, WAP and Internet settings

(Willassen 2003).

As well as retrieving data from the mobile phone, the investigators also hoped to retrieve hidden and/or deleted data from the devices. This is an interest area of this study, and what can be recovered here is a key focus in the analysis stage of the report.

FORENSIC METHODS

Mobile devices pose multiple issues that need to be addressed to ensure the integrity and reliability of forensic testing. Such issues can involve securing the data, ensuring that all possible data is recovered and other variables that could compromise potential evidence. The following will attempt to cover some

basic issues arising when forensically testing mobile devices, as well as the procedural guidelines that were established and used during the forensic analysis of the mobile devices, many of which were designed specifically to work around issues that arose or were discovered before analysis began.

Initially, all phones were given a unique identifier number. This number started at 001 and increased in increments of one for each new handset, i.e. 001, 002, 003 etc. This then ensured that each handset could be located quickly and easily and ensured that would not get contaminated.

Leading on from this, each model of handset was then profiled to determine the features and capabilities of the handsets. This was done to ensure that a variety of information was known about each type of phone All of this data was then entered into a spreadsheet with, where applicable, replications made for multiple handsets of the same exact type. This allowed easy reference for the investigators to examine the capabilities of each model of phone.

From this, testing could begin. Examiners were divided into two teams of two investigators, who would cross test all the devices across the workstations for use in the examination. For the analysis it was decided that three tests of each handset on each tool would be carried out. Initially each team would complete two tests per handset on one tool, and then the teams would swap and carry out the third test on each handset on the other tool. This ensured that integrity could be maintained because if three tests per handset per software tool provided the exact same results it would more than likely ensure that the data found was correct. This could be cross referenced by looking at the hash values generated to ensure that the value was exactly the same. It also provided integrity because it meant that it was very difficult for both teams to damage tests in exactly the same manner, which would have had to happen to provide a false positive test result.

The actual testing involved the usage of two types of data cable, one that connected the 33xx phones and another for the 51xx, 6210 and 6385 model phones. Both of these were connected via the serial port of the workstations used, these machines were IBM ThinkPad laptops, running Windows 2000. Testing involved connecting the handset to the computer and then launching the desired software. From here, analysis could occur. After all the testing was complete, the results were compiled into spreadsheets.

The investigators determined that it was appropriate to follow certain rules in the forensic investigation. This rules comprised of:

- Recording all actions/results taken
- Testing on each device is done at least 3 times by 3 different people
- Each test has to be done by 2 people, one performing actions, one recording/observing
- After data has been acquired phones are switched off
- Each investigator must perform at least 1 test per device
- Any device tested should be swapped at least once to another individual/investigator

Although the above rules are focused on working as a team, the investigators also had to research and abide by forensic methodology.

1) The mobile phone is to be switched off at the earliest possible time in order to avoid any contamination. By leaving the phone on, new data could be placed on the mobile phone, deleted or accidentally modified by the investigator
2) Each phone is to be analysed separately and software is to be closed then re-launched with every separate acquisition.
(Willassen 2005)

The investigators decided that these rules were appropriate to this study, and mobile forensics in general.

REVIEW OF MOBILE FORENSIC TOOLS USED

Forensic tools are central to the extraction of data from mobile phones. They are the interface through which an examiner can connect to a device and view and examine the available information (Geradts &

Sommer 2006). The aim of this investigation was to compare different mobile forensic software tools on Nokia handsets.

The tools utilised were chosen through reading various publications, such those from Ayers, Jansen and Schroader as well as searching the internet through sites such as www.e-evidence.info and www.phone-forensics.com. Search engines and other individuals' help and knowledge were also used to determine appropriate tools. In the end a range four tools were chosen for use, these comprising of:

- TULP 2G
- MOBILedit! Forensic
- Cell Seizure
- Oxygen Phone Manager

TULP 2G

TULP 2G is a tool developed in the Netherlands by the Netherlands Forensic Institute and is designed to examine both phone and SIM data using various plug-ins designed specifically for this program (Sourceforge.net 2006). As with many freeware tools, the user interface is not overly attractive, however it is relatively simple and easy to understand with some simple knowledge of mobile forensic techniques.

MOBILedit! Forensic

MOBILedit! Forensic is a forensic tool developed as a derivation from a program designed to operate as a mobile phone manager, it has a simple, easy to understand interface and can be used for both SIM and Phone data (Compelson Laboratories 2006). Extracted reports are protected by MD5 hashes to ensure that there is no tampering in the output. Currently MOBILedit! provides support for around 290 different types of handset which is a fairly extensive range for a lower end product.

Cell Seizure

Designed by Paraben Forensics, Cell Seizure is a tool that will analyse various types of phones as well as GSM SIM cards. It is specifically designed for forensic use and acquisition on the more popular brands of older Nokia, Siemens, Motorola and Sony-Ericson phones. The interface of Cell Seizure is very simple to use with output reports able to be created using either HTML or as a .txt file. All output is verified using a MD5 hash, which is of particular interest to the investigators, as this is a forensic testing study.

Oxygen Phone Manager

Oxygen Phone Manager was initially designed as an agent for users to edit the information stored on their handsets through their computers. However OPM has been expanded and now individually caters for Nokia and Symbian based handsets in separate versions, as well as having forensic editions designed to investigate handsets without corrupting any data on the device. Due to monetary constraints access to Oxygen Phone Manager 2 Forensic Edition for Nokia Devices could not be obtained, however a trial version of the phone manager was used for a basic idea of how OPM works. The major problem with this was that any testing carried out on handsets could not be verified, nor used in any investigation because this version was designed to allow data to be manipulated which goes against the methodology of forensic investigations.

ANALYSIS

The initial plan was to use the four tools outlined earlier to test all the handsets however some difficulties were encountered. This meant that TULP 2G could not be used at all, and Oxygen Phone Manager was used only sparingly after all other testing had been completed to ensure that the data on

each handset was not manipulated in between tests. By no means was it an ideal situation, but certain constraints prevented any other action being taken.

Another issue that arose with the testing of the phone data was that in the end, only two different types of handset could be tested for most of the phone data, these phones being the 6210 and 6385 models. Other handsets were submitted for testing that could be analysed for data, however due to an inability to gain access to the required data cables they could not be analysed in this investigation. All the other handsets that were submitted for testing were in some way able to store some sort of memory, however this was very limited and often did not contain any information such as contacts or SMS history, but merely user profiles, ring tones, logos or other information that is generally not useful from an investigation point of view.

Figure 1 below illustrates what handsets each piece of software could connect to

Phone Type	MOBILedit!	Cell Seizure	Oxygen PM
3310	X	X	X
3315	X	X	X
3330	X	X	X
6210	X	X	X
6385			X
5110/5110i	X	X	X

Figure 1 Handsets able to connect to each tool

Cell Seizure

Cell Seizure provided a somewhat reliable means for testing the handsets and returned results that were generally expected. Figure 2 illustrates what could be extracted from each type of handset.

Features Recovered	Handset Models					
	3310	**3315**	**3330**	**5110/i**	**6210**	**6385**
Contacts/Phone Book					X	Could Not Connect
SMS						
Logos	X	X	X	X	X	
Ring Tones						
Speed Dials	X	X	X		X	
Calendar					X	
WAP Settings			X		X	
Call Logs					X	
Profiles					X	

Figure 2 Output information from Cell Seizure

As can be seen the 6210 has most boxes marked indicating that it does store a lot of data in the phone memory and more importantly, that Cell Seizure is able to extract this data from this handset. However the 6385, a CDMA handset could not connect to Cell Seizure due to issues with the program not providing support for this particular model.

MOBILedit! Forensic

Every device except the CDMA 6385's could connect to MOBILedit! With this tool, the table below needs an explanation. MOBILedit! was able to demonstrate if there were contents, i.e. missed calls, but it actually recovered none from the phone, meaning it has the capability to do so, just there was no actual data for this type on any of the phones tested. Figure 3 shows exactly what information could be extracted from each different type of model.

Features Recovered	Handset Models					
	3310	**3315**	**3330**	**5110/i**	**6210**	**6385**
Contacts/Phone Book	X	X	X	X	X	Could Not Connect
SMS	X	X	X	X	X	
Logos						
Ring Tones						
Speed Dials						
Calendar	X	X	X	X	X	
WAP Settings			X			
Call Logs	X	X	X	X	X	
Profiles						

Figure 3 Output information from MOBILedit! Forensic

What is most interesting here is that the Nokia 3330 actually had a wider range of data recovered than the 6210, even though the 6210 supposedly should store more information. This could only really be put down the operations of MOBILedit!

Oxygen Phone Manager

Oxygen Phone Manager was only used in a very limited format because of its ability for the investigators to potentially erase data from the handsets. In the event the forensic edition had been acquired then full use would have been made of this program, but the risk of erasing data was too great. Oxygen Software list over 130 different models of Nokia phone that are compatible with the Oxygen Phone Manager 2 Forensic Edition for Nokia Phones. One of which is the 6385, a model that could not connect to either MOBILedit! or Cell Seizure, so the testing on OPM purely centred around what could be displayed from the 6385 CDMA model phones. The following are the areas of interest that produced results to the investigators:

- Contacts/Phone Book
- Calendar
- Profiles
- Logos
- Call Logs
- SMS
- Voice Recordings

OPM was a simple and manageable tool to use. It displayed all data in a simple and clear format. It seemed to be quite extensive in its findings. The above list was quite extensive, giving a vast amount of data to analyse, which is an advantage. OPM did give the investigators an opportunity to investigate CDMA phones, which was a great advantage. Although this study is somewhat focused on GSM devices, it was important to investigate CDMA phones. Please see Log of Event forms for details on OPM details.

TULP 2G

TULP 2G was unable to be used in this investigation unfortunately due to reasons outside of the investigators' control. The Windows 2000 based laptops provided were part of the university and although being specially programmed for this investigation, when installing TULP 2G an error would occur regarding administrative access and could not be resolved. Furthermore on Windows XP based machines TULP 2G would not connect to Nokia handsets. The docking station used to connect to the 3310/3315/3330 models would not even be identified on XP machines.

Functions Performed

An important aspect of this study was to gain an understanding of the promises of the particular software tools, and what they actually delivered. The investigators selected the particular pieces of software based on what functions the developers promised the tools would perform. In reality, certain tools did not carry out functions that they were advertised to execute. This was certainly a let down for the investigators, because the research on the tools performed was reasonably extensive and these were selected due to their supposed capabilities.

Promised Results	Tools			
	TULP 2G	**OPM**	**MOBILedit!**	**Cell Seizure**
MD5	Unknown	Unknown	Not Found	Yes – Unreliable
SHA1	Unknown	Unknown	NA	Not Found
Reports - HTML	NA	Unknown	NA	Yes
Reports – XLS	Unknown	Unknown	Yes	NA
Reports – XSL	NA	NA	Yes	NA
Reports – CSV	NA	Unknown	NA	NA
Reports – XML	NA	NA	Yes	NA
Reports – RTF	NA	Unknown	Yes	NA
Reports - TXT	Unknown	Unknown	Yes	Yes
Compatibility with Windows	XP, unknown others	2000, unknown others	2000, unknown others	2000, unknown others
GSM	Unknown	Yes	Yes	Yes
CDMA	Unknown	Yes	Beta Support	Incompatible with 6385
Backup	Unknown	Unknown	Yes	Yes

Figure 4 Output of Software Tools

Figure 4 above shows the returned features of the software tools used as compared to the promised features from the manufacturers. This demonstrates that some manufacturers fail to deliver some promised features under our test conditions. The most disappointing aspect was the difficulty in finding the MD5 hash values using MOBILedit! and the SHA1 hash values in Cell Seizure. The investigators extensively searched the software for these, but were unable to locate the values. Although versions of software change periodically, every care was made to locate these values, but it could not be done. The Yes- Unreliable score regarding the Cell Seizure MD5 hash values is explained in the Results section of this report.

As a guide for the table above Unknown relates to features that were said to be available on the tool, but could not be utilised through a lack of access to the tool for various reasons (see individual software analysis). NA indicates that feature was not available on that individual tool. Yes means that the feature was promised, and was delivered. CDMA compatibility with Cell Seizure could not be determined because only one model was submitted for testing; this model was not compatible with Cell Seizure.

RESULTS

Overall the results gathered are quite interesting, however for privacy reasons, the disclosure of the actual data and information recovered can not be given out. The HTML report Cell Seizure is capable of producing was found to be useful when re-examining previous test data because it was displayed in such a way that individual areas of interest could be found quickly and easily. Also the MD5 hash was simple to locate (due to it being displayed in a HTML report) and did not require extensive effort to

discover. This overall professionalism would certainly make presentations much easier for general observers to understand.

With regards to the Nokia 6210, Cell Seizure and MOBILedit! both retrieved data from the contents of the device. MOBILedit! displayed the text messages from the Nokia 6210 and although this data is arguably the most important in an investigation, Cell Seizure recovered much more data. Further information recovered from the 6210 using Cell Seizure included Profiles, WAP profiles, logos and Call logs. Cell Seizure did not manage to recover the text messages stored on the device's memory, whereas MOBILedit! did, but in the same sense MOBILedit! could not recover the call logs where Cell Seizure could. From this it can be determined that no tool is really better than the other, because they both extract different information. Although in certain instances this may be seen as a hindrance due to time and/or financial constraints. This could also be an advantage because it means that more tools may need to be used to recover the target data, but in the process these tools may extract other information that may otherwise not have been found.

Cell Seizure MD5 Hashes – HTML Reports

When analysing the MD5 hashes from Cell Seizure, some anomalies arose. After each test, the MD5's were analysed. These were checked and seen that they are all the same. It was at a later point when the investigators were writing the report that they realised that the MD5 hashes generated in the HTML reports were the same between different handsets.

Immediate tests were carried out in order to prove the integrity of the findings. This again showed that some models of phones retrieved the same MD5 hashes as each other. The Nokia 5110 and the Nokia 5110i produced the same MD5 hash. These phones produced exactly the same results, 1 logo retrieved off its memory. The only explanation the investigators' can give for this is that because the handsets are both older and do not contain vast amounts of memory, the only item returned was the logo, the MD5 calculated only hashed the information retrieved from the phone and not and of the individual phone data such as the IMEI. If information such as the IMEI was included in the data that was to be hashed the value returned would surely be different unless an error in the hashing occurred. Also, the logo retrieved on both phones would have been a factory setting, and uniform amongst all phones, so the report generates its MD5 sum from the contents of the phone, not the whole phone itself.

The same scenario occurred with three Nokia 33xx phones. Each returned exactly the same MD5 hash as each other when displayed in the HTML reports. These phones comprised of two Nokia 3315s and a Nokia 3310. It was after each phone was individually tested and the results tabulated that it was discovered that the MD5 hashes were the same. All of these retrieved the same data as each other, but they still should have returned different MD5 sums. Interestingly, the Nokia 3330 tested retrieved a different MD5 hash as the phones above. Possible reasoning for this include that the Nokia 3330 has WAP capabilities, signifying that the information stored would not be entirely factory information.

After it was discovered this had occurred, the investigators went back and traced the IMEI number of the phones, to ensure that they had not executed the testing incorrectly. The IMEI numbers of each phone are completely different to each other, ensuring that they are all different phones. The investigators can prove that they tested seven different phones, because each has a different IMEI number to each other.

Whilst this issue should not arise in newer handsets due to larger onboard memory capabilities and hence the ability to store more information, it cannot be definitely ruled out that this may not occur in future tests. More than likely however this is simply a case of what has been stated above and the data that was hashed did not include identification information about the handset. This could also be located to a flaw in the software that prevents it from outputting a hash of the phone memory itself. The

following tables illustrate the MD5 hash collisions that were generated in the reports, this duplication was not limited to the handsets shown here, other handsets also produced duplicate MD5 hashes.

Phone 001 – Nokia 3315

Test Number	MD5 Hash	Model IMEI
Test 1	530dcf6a49d447051b4e48db0634aaa8	351454301860957
Test 2	530dcf6a49d447051b4e48db0634aaa8	
Test 3	530dcf6a49d447051b4e48db0634aaa8	

Phone 014 – Nokia 3310

Test Number	MD5 Hash	Model IMEI
Test 1	530dcf6a49d447051b4e48db0634aaa8	350114303886050
Test 2	530dcf6a49d447051b4e48db0634aaa8	
Test 3	530dcf6a49d447051b4e48db0634aaa8	

Phone 5110i – Nokia 5110i

Test Number	MD5 Hash	Model IMEI
Test 1	0497703b5324f3f946bbcceddc269cbf	350010300204182
Test 2	0497703b5324f3f946bbcceddc269cbf	
Test 3	0497703b5324f3f946bbcceddc269cbf	

Phone 008 – Nokia 5110

Test Number	MD5 Hash	Model IMEI
Test 1	0497703b5324f3f946bbcceddc269cbf	449217300841367
Test 2	0497703b5324f3f946bbcceddc269cbf	
Test 3	0497703b5324f3f946bbcceddc269cbf	

Cell Seizure Hashes – Varying Hashes

Upon investigation for the SHA1 hash values from Cell Seizure, it was discovered that the MD5 values were different to the values generated in the HTML reports. For every test of each handset, Cell Seizure stores a copy of the results in the "Cell Seizure directory", e.g. C:\Program Files\Paraben Corporation\Cell Seizure, as well as allowing the user to choose a specific location where the backup and report files will be saved.

When searching the files in the Cell Seizure directory, there are four files saved for each test. These are a .VIW, .VRS, .CSZ.MD5 and a CellSeizure document. The VIW files are of no interest, with the Cell Seizure document being the backup of the test results. It is the VRS and MD5 files that the hold key information. Each of these files stores a 32 character alphanumeric string. The issue concerned arises when comparing these numbers. The VRS string stores the exact same string in each .VRS file, no matter what handset or test number the file name relates to. For this investigation all files were named in the same format of XXX-Y where XXX represents the handset number and the Y represents the test number. It was originally thought that this was the SHA1 hash value, however with this issue it would be highly unlikely that it is the SHA1 value. This had been ultimately ruled out after examination from the Project Supervisor.

The second problem from this directory arises with the .CSZ.MD5 files. The 32 character alphanumeric string saved in each of these files is different to every other file with the same extension. The problem is that it is also different to the values generated and displayed in the HTML reports that Cell Seizure produces, and is a different value for each test case stored in this directory.

In effect, for a handset tested 3 times on Cell Seizure, there is a return of four MD5 hash values. The only conclusion that the investigators could determine was that the values generated in the reports were the same because they did not include the timestamps in the hash calculation, whereas the values generated in the .CSZ.MD5 files hashed all of the data including the timestamps and thus created a completely different value. It is extremely unlikely that an MD5 hash value can ever be the same as

another, because if it has a different timestamp, i.e. performed at a different time. This could potentially create a large problem because it opens a door whereby it could be argued in court that since the hash values differ, then the testing could be corrupt. The only way to prove otherwise is to determine exactly how each file is generated in the program. The results taken from the relevant files are displayed below to illustrate these findings. This is only part of the results found, however all other tested devices produced similar results.

Phone 001 – Nokia 3315

Test Number	MD5 Hash	Model IMEI
Test 1	03b261e2b2a9c57ca3c5fc0ee8b24c59	351454301860957
Test 2	201c5d87c214e19401938e9910027079	
Report	530dcf6a49d447051b4e48db0634aaa8	

Phone 014 – Nokia 3310

Test Number	MD5 Hash	Model IMEI
Test 1	c5866f60b3487aae42f735470b64aa95	350114303886050
Test 2	558f7b747a5b818e123586935fdf8776	
Report	530dcf6a49d447051b4e48db0634aaa8	

Phone 5110i – Nokia 5110i

Test Number	MD5 Hash	Model IMEI
Test 1	Bdad3c583c494c471f55624e1128ca51	350010300204182
Test 2	d803b9cd63855487ee978bfc08aefbd7	
Report	0497703b5324f3f946bbcceddc269cbf	

Phone 008 – Nokia 5110

Test Number	MD5 Hash	Model IMEI
Test 1	4316fb7ee961605b6506dc9c366a22b4	449217300841367
Test 2	5c8e19bb41d55d9f24cb49b2b7b4ccbe	
Report	0497703b5324f3f946bbcceddc269cbf	

Upon these findings, the investigators determined that the MD5 function in Cell Seizure is very inadequate. It assigns four different MD5 values for three different tests. The individual MD5 hashes for each test are hidden away in software directories, making it difficult for some users to locate. It is much easier for the user to generate the MD5 value through the HTML or TXT reports that can be gained through a very simple wizard. It is clear that the MD5 hash value is unreliable, with the fact that Cell Seizure advertised that it also performed SHA1 hashing, which the investigators failed to locating, indicating that it is highly unlikely that Cell Seizure does not perform this.

ISSUES UNCOVERED IN THE RESEARCH

Some major issues arose during the analysis stages of this investigation. The primary issues are outlined above and, where possible, reasons to why this occurred are provided through the extensive research that followed once the issues occurred.

Call Logs

The call logs on most GSM phones cannot be recovered once a new SIM card has been inserted into a GSM handset. This is explained in further detail in (Cheam et al. Unpublished Paper) however essentially what occurs is that the call logs, which store the received and missed calls as well as outgoing calls, are reset when a new SIM card is inserted into a handset. In the event that one particular SIM card is removed from the handset and then replaced back into the handset without any other SIM card being inserted into the handset in between then that memory will not be erased, but the moment a different card is inserted the call logs are erased. This was a huge problem because the investigators did

not have access to the previous SIM cards so could not extract this data. Alternatively the SIM cards submitted for testing were not connected to networks so no call logs could be created as such. The only call logs handsets that the call logs could be technically extracted from were the 6385 CDMA devices.

Deleted Data

Extracting deleted data from the handsets was impossible in this investigation. There are no known forensic software tools currently available that deal with "un-deleting" or recovering deleted data from mobile handsets. The only widely known possible method of extracting this data from handsets is to firstly image the memory from the handset to a computer and then forensically analyse the image using tools such as Encase to extract the data. It is stated in Willassen (2005) that "It is impossible to recover deleted items" from the internal contents of a mobile phone. This was simply too far out of scope of this investigation but would certainly be a major area of interest for future investigations into mobile phone forensics.

Network Connectivity

Due to the nature of mobile phones they are almost always on and connected to a network, this means that messages can be sent and received and calls also sent and received. The first step once a mobile handset is seized should be to protect that handset from the network to ensure that new data cannot be sent to, or from, the device which could change the memory from the time of seizure and potentially delete other data that could be used as evidence. To secure devices this way they should be immediately switched off to prevent access to the mobile network. When turning the device back on, a faraday bag, or other similar apparatus should be used to prevent the device from connecting to the outside mobile network. This however was not a major issue in this investigation because all devices submitted for testing were not to be tested from a law enforcement perspective, merely an analysis of what could be extracted. Some problems did arise however when SMS messages were received by some SIM cards from the network carrier and it highlighted the need that these sorts of precautions really should be taken in a real world situation.

CONCLUSION

Overall the investigation could be classed as a partial success. The investigators did not retrieve any deleted data from any mobile devices. Some information was found using the MOBILedit! and Cell Seizure tools but in an ideal world this would have been able to be compared against other forensic tools such as the Oxygen Phone Manager Forensic Edition, TULP 2G and even other higher priced software. University monetary constraints did play a role in preventing this from occurring, these same constraints also prevented a lack of access to newer more relevant handsets and the associated cables, but this did allow a lot of focus to be placed upon some older handsets that may not otherwise be generally looked at in other studies.

The research presented in this paper highlights issues that forensic investigators need to be aware of when testing mobile devices. Further research regarding the MD5 hash values and other mobile forensic software should be encouraged to enhance knowledge within this field and to reduce the risk of software inadequacies. Such examples of further research could include testing of md5 hashing in regards to electronic devices, in-depth analysis of specific forensic software programming to reduce inconsistencies and environmental impacts of forensic testing. These research areas should not be limited to mobile phones alone, but all electronic devices in general.

Forensic Investigators should be made aware of testing procedures that will ensure the integrity of the data. Research into this area is minimal at the present and further discoveries can be made with time. Investigators that fail to comply with validated testing procedures can face serious consequences in regards to ensuring the integrity of their findings. Further research into testing procedures would

hopefully result in a uniform set of testing procedures for all tests, and possibly being standardised. As this area is quite immature, the efforts made currently are not fully guaranteed.

REFERENCES

Compelson Laboratories. (2006). *About MOBILedit! Forensic,* URL from http://www.MOBILedit!.com/forensic/ Accessed 28 September 2006.

Cheam, B., McDonald, M., Williamson, B., Apeldoorn, P. (Unpublished Paper). Analysis on Forensic Tools of Subscriber Identity Modules.

Ciao GmbH. (2006) – *Nokia N91.* URL http://www.ciao.co.uk/Nokia_N91__6347857

Accessed 28 October 2006

Geradts and Sommer. (2006). *Future of Identity in the Information Society,* URL http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf Accessed 19 October 2006

McCarthy, P. (2005) *Forensic Analysis of Mobile Phones*, URL http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf Accessed 17 October 2006

Oxygen Software (2006). Oxygen Software :: *Oxygen Phone Manager II (Forensic version,* URL http://www.opm-2.com/forensic/ Accessed 8 October 2006.

Paraben Corporation (2006). Paraben Forensics - *Forensic Software, Hardware, & Training,* URL www.paraben-forensics.com/index.html Accessed 14 September 2006

Sourceforge.net. (2006). *TULP2G,* URL http://tulp2g.sourceforge.net/ Accessed 4 September 2006

Willassen, S. (2005) Evidence in Mobile Phone Systems, URL http://www.mobileforensics.com/

Accessed 13 September 2006

Willassen, S. (2003) *Forensics and the GSM mobile telephone system.* URL www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf Accessed 29 August 2006

COPYRIGHT