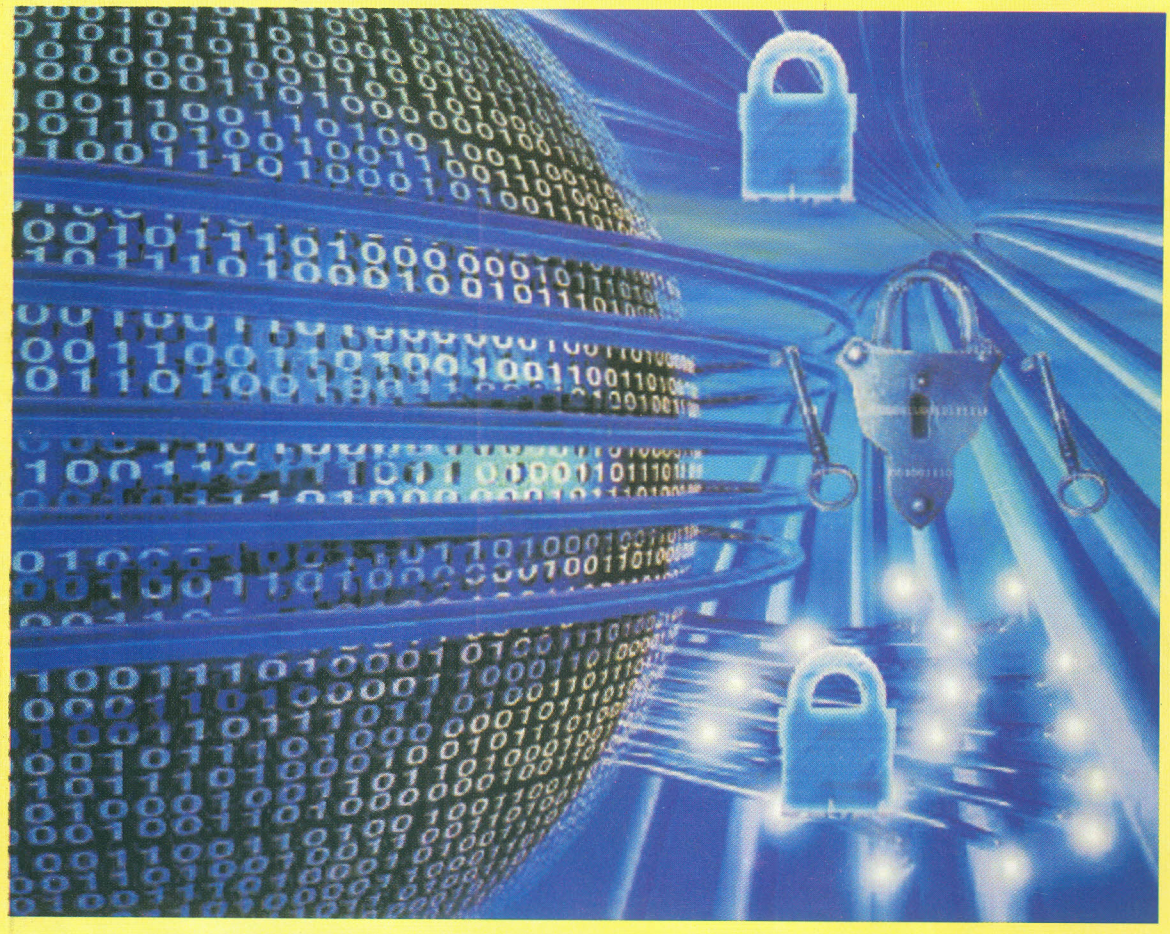
ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics



Mobile Forensics

3

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

– इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

—Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics

Block

3

MOBILE FORENSICS

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writer

Ms. Sugandh Agarwal
Ocean Technocrats
Noida
(Unit 1, 2, 3 & 4)

Block Editors

Prof. Ajith Kumar R, Professor
Indian Institute of Information Technology and Management-Kerala (IIITM-K)
Trivandrum, Kerala

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

Feb,2012

ISBN-978-81-266-5924-1

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed at: Berry Art Press A-9, Mayapuri, Phase-I New Delhi-64

BLOCK INTRODUCTION

This block deals with the mobile forensics. It is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field. A proliferation of phones on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques. This block comprises of four units and is designed in the following way;

The **Unit one** deals with the "Introduction to mobile forensics and technologies". We covered Mobile Forensic Tools and data stored in Mobile phones in detail. We discussed Extracting data from Mobile phones, from SIM Cards and from phone memory.

The **Unit two** deals with the "Analysis of CDR's". Call Detail Record (CDR) can contain information that the mobile network operator uses for subscriber identification, call charging, services obtained, call routing etc. It also covers types of Call Data and explained SIM Card Analysis and SIM Characteristics.

The **Unit three** covers "Aplications of SIM card reader's". The Synopsis of SIMIS, Synopsis of ForensicSIM, Synopsis of Forensic Card Reader, Synopsis of SIMCon are discussed in detail.

Unit four explains forensic examination of mobile devices. While most toolkits support a full range of acquisition, examination and reporting functions, some tools focus on a subset. Similarly, different tools may be capable of using different interfaces (e.g. IrDA, Bluetooth, or serial cable) to acquire device contents. The types of information that tool can acquire can range widely and include PIM (Personal Information Management) data (e.g. phone book); logs of phone calls; SMS/EMS/MMS messages, e-mail, and IM content; URLs and content of visited Web sites; audio, video and image content; SIM content and uninterrupted image data.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INTRODUCTION TO MOBILE FORENSICS AND TECHNOLOGIES

Structure

1.0 INTRODUCTION

These days mobile phones constitute one of the most commonly used electronic devices. In this context, one should also mention that the mobile communications market is one of the largest growing markets worldwide. Amongst all available mobile communication technologies, it is the GSM standard which dominates with a share of 75% of all mobile phones. Global system for mobile communications (GSM) is used in 200 countries and holds more than 1.2 billion subscribers in more than 630 networks.

Today's mobile phones combine a variety of different technologies. That is why they offer in addition to excellent mobile availability and connectivity also high speed data transfer via universal mobile telecommunications system (UMTS) and wireless local area network (WLAN) for the user. Moreover, they are multimedia capable due to their integrated digital camera or music player and not to forget, they serve the function of text-based communication via e-mail, multimedia messaging service (MMS) and short message service (SMS). Consequently, they are used increasingly as a 'mobile office', thanks to the various office applications available for mobile phones. Another aspect which should not be neglected is the fact that current mobile phones are more frequently equipped with GPS-Modules which enable the user to make use of the mobile phone for navigation purposes.

By means of the above stated quantity of data and the continuously increasing number of criminal actions in which mobile phones play an essential role, not only for the criminal action itself but also within the investigation of those, it becomes evident how important the classification, the backup, as well as the recovery of a mobile phone's contents are.

A digital investigation is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Although there are already tools existent which are able to extract evidence, it cannot be denied that there is a huge demand to develop more sound forensic procedures and tools in order to analyze data from a previously created dump, as well as from the mobile phone itself.

Such a developed tool should enable the process of loading a memory dump which was previously created, with the help of Twister Box or a software agent running under Symbian OS on the phone. The data retrieved this way, which are dependent on the producer and are available in coded form, will be subsequently converted into plain text to finally draw conclusions about the relevance of the content in the context of forensic analysis.

Within all those operations a set of principles guiding the process were suggested and are quoted below.

- No actions performed by investigators should change data contained on digital devices or storage media.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- An audit trail or other record of applied processes, suitable for independent third-party review, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- understand various aspects of Mobile Forensics; and
- explain different scientific methods followed in investigation.

1.2 INTRODUCTION TO MOBILE FORENSICS

First of all, we must pay attention that the mobile phone is prevented from establishing a connection neither to its provider nor to another than the chosen computer as not to change any data during analysis.

We will now outline some of the currently existing software solutions and contrasts its strengths and weaknesses.

1.2.1 Dumping the Memory

After preventing the mobile phone from establishing a connection to the network, we can start with the analysis of the smartphone. The first step is to create a dump of the mobile phone's memory. The existence of different operating systems necessitates varying procedures in order to create a memory dump. In the following sections we present the different procedures for both, older Nokia mobile phones and Symbian devices.

Twister Box is a complete kit for removing simlock and servicing such phone series such as Nokia DCT3, Nokia DCT4, WDT2/EPOC, TIKU BT2, DCT-L, Samsung, Sony Ericsson or Motorola and Acer. It allows us to repair all bugs within the software such as Bluetooth error, no service, contact provider or illegal software loaded. Of course, it can also be used for removing security code, phone code and change software or language or upload Java applications.

The Box contains an atmega8 chip1 with the system files and a ftdi-232bm2 chip for communication purpose between the mobile phone and the investigator's computer. The box supports two communication modes, the 1A 8-bit AVR micro-controller with 8K bytes in-system programmable flash build by ATMEL Corporation.

The FTDI 232BM USB to Serial UART interface chip converts USB to serial data (I/O's at TTL levels). All USB protocols are handled in the chip, so no knowledge of USB is required. The 'FBUS mode' for gathering phone information and the 'flash mode' for direct communication with the mobile phone flash chips. However, in case of this diploma thesis we use the working technique of the Twister Box to create memory dumps with the help of the flash mode of the attached mobile phones.

A memory dump created with this technique is available in PM format. In this case, data are pre-formatted and their hexadecimal representation is saved block by block as a PM file. One can find an unambiguous number framed in square brackets can be found. Based on this number we are able to draw conclusions about the content of this block. Such a block can incorporate several indexed entries which in each case occupy one line of the file. The 'real' entry is separated by '=' from its index and arranged byte-by-byte.

Within the device the HEX-Value 0x02 takes exactly one byte whereas the value within the PM file consists of the signs 0 and 2 which count for more than one byte.

The entries occur repeatedly and can incorporate a constant structure.

1.2.2 Symbian Software Agent

In order to analyze data of a Symbian phone various approaches exist. The most common approach includes the use of command-respond protocols like the AT Command Set, OBEX or the FBUS owned by Nokia.

Those protocols are already implemented on the Smartphone and allow the investigator an easy use as they are contained in many SDKs and thus are well documented in most cases.

Disadvantages of those protocols lie in the fact that on the one hand we have to trust the correct implementation on pages of the Smartphone. Therefore we cannot assure that the 'answers' which are sent by the telephone after requests of the investigator are consistent with the contents of the desired storage space. 232BM is entirely state machine based and no firmware is required. Supports baud rates of up to 3 MBit/second.

On the other hand, those protocols change data on the phone. Does the investigator, for example, wish to receive the SMS messages from the incoming box of the smartphone, then unread message are sent to the PC of the investigator, but they are afterwards marked as 'read' in the incoming box of the smartphone.

This procedure is not acceptable according to forensic principles.

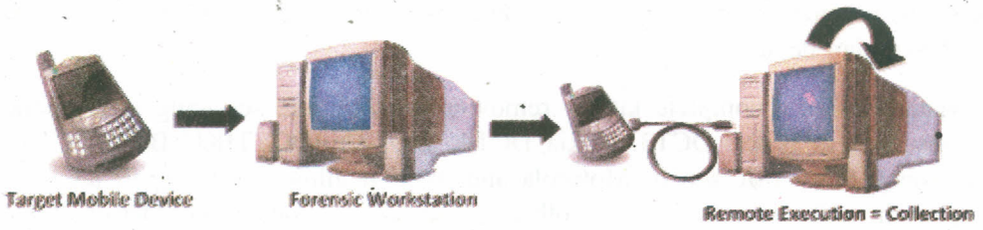


Fig.1: The classic client-server workflow

A direct improvement of this procedure offers an On-Phone forensic tool, also known as Symbian Software Agent. This agent is a small program which has to be installed on the smartphone to be examined. This tool allows data exchange and connection establishment between PC and smartphone with own protocols. This approach uses client-server architecture, by which the smartphone operates as a server. Here we need not trust the connectivity services which are provided by the manufacturer. A disadvantage of this procedure is that the tool has to be installed on the device, here data become changed.

Those data changes can be narrowed down when using modern agents. Then, the tool is installed on a memory card instead on the internal storage of the device. However, with this approach it is also worked directly on the phone within the whole analysis (see Fig. 1) and there is no possibility of creating a memory dump.

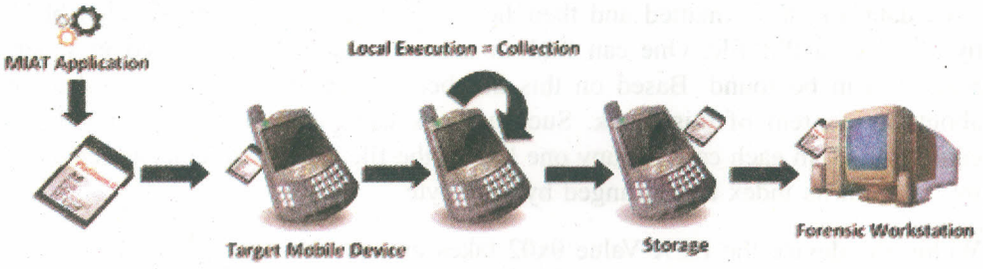


Fig. 2: The MIAT workflow

The second approach of a software agent which is currently available is shown in Fig. 2. Here, the agent functions as a tool for creating a memory dump of specific, for the analysis important, files of the internal storage of a smartphone.

This approach has been implemented in the tool MIAT of the University of Rome. For this purpose we copied MIAT to a memory card which we afterwards inserted into the phone. After the installation of the agent we can now create an exact dump of private data on the phone. Within this process the security restrictions are circumvented as far as possible in order to gain private data.

The backup we created in this way is stored on the memory card in order to guarantee that no other data have been overwritten on the phone. After a successful completion of the backup process we can remove the memory card and we can conduct the complete analysis on the memory dump. In order to prove the integrity of saved data afterwards, we formed hash-sums from the single files. Those are stored in a log file then.

Again, we have to mention the disadvantage that changes are done to certain parts of the phone due to the installation of MIAT. Moreover, the analysis as well as the processing of data and data formats is completely put into the responsibility of the investigator which implies the need for a certain level of knowledge of the latter.

1.2.3 Windows CE

The two main classes of data extraction techniques on Windows CE running devices are either logical extraction or physical extraction. A logical extraction technique focuses on the visible content at the file system level only, i.e. data pertaining to files, databases and registry along with other file system data.

MIAT-WM5 is a promising logical data extraction tool for WinCE running on PDAs and smart phones. A physical extraction technique, on the other hand, is attractive because it can recover all data stored on an electronic device. In most cases, however, only the flash ROM and the RAM content are recovered by using a special operating mode of the device or by communicating with the operating system.

According to Breeuwsma et al., three techniques may be used to obtain a complete copy of flash memory: (i) using flasher tools, (ii) using JTAG test access ports and (iii) using forensic de-soldering.

Flasher tools are designed to copy the memory of certain families of electronic devices. They employ APIs that interact with the addressable memory. Generally, these tools originate from manufacturers, who use them for debugging purposes or they come from the hacker community, which creates the tools to modify the functionality of handheld devices. An important advantage of this technique is that flash memory can be imaged without de-soldering the chip. However, many flasher tools do not make complete forensic copies of flash memory, mostly because of the limited functionality of the API provided by the embedded device. To state an example of flasher tools we point out to the Twister Box.

The second physical extraction method involves the use of JTAG test access ports of embedded devices. JTAG ports in most devices are designed for debugging purposes, but they can also be used to access the flash memory. The JTAG extraction technique is complex and time consuming; however, it is possible to guarantee that no data are written to memory during the data recovery phase.

The third physical extraction technique is to de-solder the memory chip and use a chip programmer or reader to extract the data. This method is expensive, time consuming and the most invasive but it can be used to recover data from damaged devices, too.

1.2.4 OS X iPhone

An Apple Support knowledge base document describes the various procedures and limitations of a backup of data on an iPhone. Due to the OS based implementation of Digital Rights Management (DRM), we can only save certain data in the way it has been described by Apple.

While limited portions of personal data can be viewed and saved this way, more hidden and ostensibly deleted data are available by examining the raw disk dump. That information stored by the iPhone includes, according to Zdziarski

- **Keyboard caches** containing usernames, passwords, search terms – nearly everything typed into the iPhone's keyboard is stored in this cache.
- **Screenshots** are preserved of the last state of an application, taken whenever the home button is pressed or an application is exited.

- **Deleted data** like voicemail recordings, address book entries or images taken by the camera or even out of the browsing cache.
- **Call history** with about 100 entries can be restored through the call database including deleted calls.
- **Google Maps** searches and images including GPS coordinates can be recovered also.
- **Browser cache** and deleted browser objects.
- **Messages** like e-mail, SMS and other communication can be recovered including timestamps and flags.
- **Pairing records** establishing trusted relationships between the iPhone and one or more desktop computers or other handhelds can be recovered.

According to Varsalone, three possibilities to create a memory dump of an iPhone exist. We explain these in the following:

- **Viewing the iTunes Sync on a host computer:** it is possible to obtain a logical copy of iPhone data with the help of an iTunes Sync Tool. However, within this memory dump are only non-DRM-protected data contained, as long as the Sync is not conducted with the host computer of the suspected. Admitttedly, even then it is not possible to dump deleted or hidden data.
- **Hacking into the iPhone:** it is possible to hack the iPhone with the help of jailbreaking5 in order to use UNIX tools like dd and ssh afterwards as to conduct a complete bit-by-bit-copy via the WiFi-connection. A disadvantage of this technique is constituted by the fact that when dealing with iPhones in many cases6 the firmware has to be changed in order to install the jailbreak software (e.g. Pwnage) which in effect leads to changed data on the phone. After we have successfully installed Cydia, a UNIX toolkit for the Apple iPhone, we are able to dump the complete user data partition byte-by-byte on a host computer with the command shown in below Listing

```
dd if=/dev/ di sk0s2 conv=sync , noerror bs=4k j nc??w1 <ip address of host pc> 26000
```

Listing : Command for dumping the iPhone memory

The dd-file we created this way can be altered to a dmg-file on a Mac OS X computer and simultaneously mounted to a read-only file. Afterwards it can be worked on it in the same way as on a hard disk. With the help of tools like X-Ways or BlackBag we can conduct a data analysis in a forensic sense.

- **Disassembling the iPhone:** All ROM chips must be de-soldered from the iPhone. Then the data contained must be saved with the help of a NAND dump. Here it holds also true that this method is expensive, time consuming and the most invasive one.

1.2.5 Selection of Existing Tools

When the creation of the memory dump has been completed, we can now analyze this dump with the help of some commonly used software solutions. In this section, we discuss these tools as well as solutions for analyzing the mobile phone's data directly.

- Gammu

The first tool we present within this section is called Gammu. This tool had been previously known as MyGnokii2. It is available as open-source and is the only

tested tool which operates platform-independent. Offered are many The term 'jailbreaking' originates from a UNIX practice of putting services in a restricted set of directories called a 'jail'. Many iPhones used in Germany have already installed a jailbreak firmware as to use those phones also in mobile phone networks other than T-D1. In this cases the changed data through the investigator is very small extensions to the tool, e.g. a graphical interface like 'GammUI' or 'Wammu'.

Moreover, thanks to a Python module, the possibility exists to develop new extensions for Gammu on one's own account in order to implement new functions or to adapt the tool to one's personal needs, as well. Amongst many Linux distributions Gammu and Wammu are already included within the repository to facilitate installation.

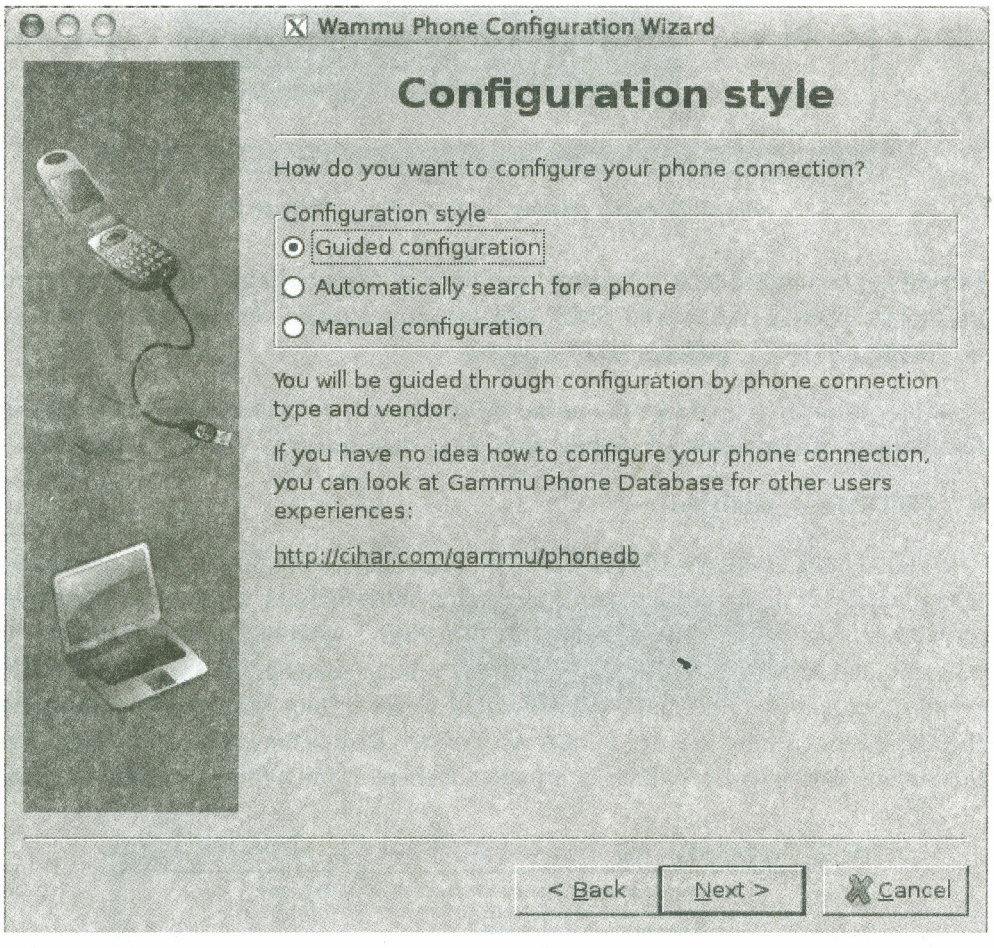


Fig. 3: Wammu phone configuration wizard

To ease the configuration of the mobile phone extension the user can make use of an assistant within the graphical interface (see Fig. 3), which recognizes the mobile phone connection, either manually or fully automated. Thereafter the configuration file of Gammu is adapted. However, we have to mention that a high degree of professional knowledge is needed. The investigator is forced to open and use the assistant when opening Wammu (see Fig. 4).

The tool offers support for a broad range of mobile phones and due to the huge developer community the list of supported mobile phones is constantly enlarged.

A disadvantage of this tool constitutes the fact that it directly operates on the mobile phones rather than on the memory dump. It uses the communication via F-/M-Bus when dealing with Nokia phones and via AT-commands when dealing with other manufacturers. Moreover, it actively supports changing data on the mobile phone which does not allow for a sustainable line of argument.

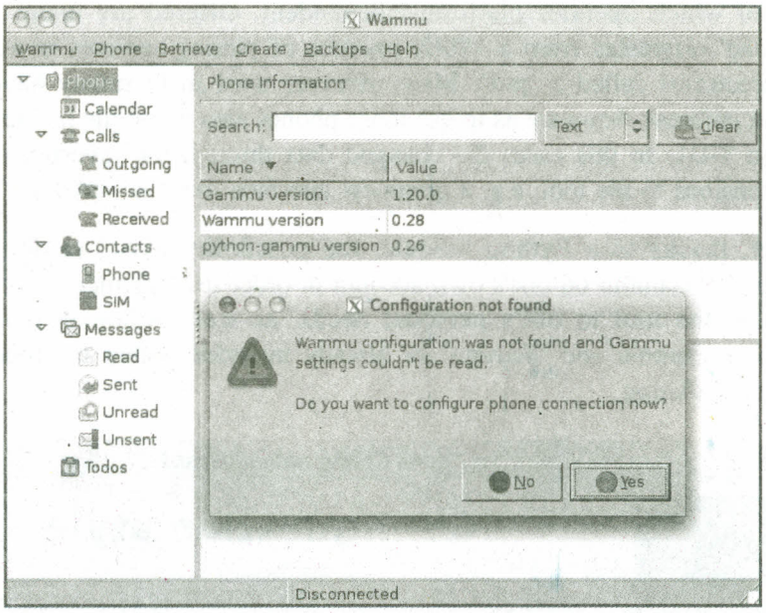


Fig. 4: Wammu missing configuration at first start

During the conducted tests it became obvious that Gammu found many data stored on mobile phones like 'saved SMS' and directory entries. Though, unfortunately no 'cached SMS' or pictures were detected.

As a last point we would like to outline that the above described tool is not suitable for forensic investigation of mobile phones as data integrity cannot be assured.

- **Cell Phone Analyzer**

The Cell Phone Analyzer (CPA) from BK-Forensics tool offers a clear and easy-to-use interface, allowing also inexperienced investigators to conduct a mobile phone analysis. This fact becomes evident in Fig. 5 when selecting the device to be examined and the image type. CPA offers a huge selection of supported mobile phones. Moreover, in contrast to many other tools, it does not operate directly on the device but rather on the dumps of Twister Box. This method of operation guarantees data integrity which is a major concern from a forensic point of view.

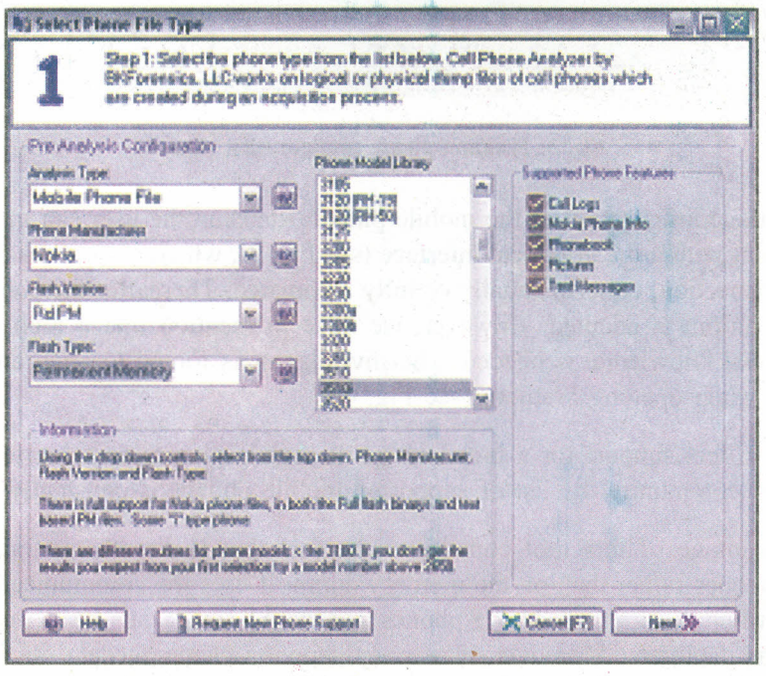


Fig. 5: CPA select phone and file type for analysis

In addition, CPA offers a detailed report function which can be adapted to the needs of each individual investigator with the help of the Report Wizard. To state some examples, the investigator's name, date, company or a reference number can be deposited which then appear in both, the report and the analysis file. The actual report can be created in various formats (e.g. HTML, text or rich-text). Moreover, the report directly shows the offsets of found and decoded data in order to make the procedure more transparent.

Random DOTS placed in output during DEMO mode

Nokia SMS Data [7 records found]	
DESCRIPTION:	
Items	Data
Rec# 1 Active	
Offset (Hex)	60..255 [000015CB1]
Folder	Outgoing
Status	Sent
Date	.4/22/2009..9:34:59
Number Type	International
Number	491703.0.447
Origin	Sender
Number Type	International
Number	491..0.50440
Origin	SMSC
Message Text	Die. ist .ine..ext-SMS!

Fig. 6: Excerpt of the CPA report for SMS

After we have done a detailed analysis of the report, it becomes evident that the tool has found many data on the mobile phone (e.g. SMS, cached SMS, the register, the call history and general smartphone information as depicted in Fig. 6). However, we must also point out that the tool does not find any stored pictures although those exist on the phone. Due to the fact that within this diploma thesis only the demo-version had been available the report contains random dots. However, there are no restrictions concerning the functionality of the tool as compared to the full version.

Nokia Phone Information				
DESCRIPTION:				
Rec#	Offset [Hex]	Record Name	TagID (FBUS only)	Data
1	1.387 [00888378]	System Info	Production Serial Number Active	968.66.69
2	1.387 [00888378]	System Info	Product Code Active	0.10.100
3	1.387 [00888378]	System Info	Basic Product Code Active	0516..30
4	1.387 [00888378]	System Info	Module Code Active	0.0.9110
5	1.387 [00888378]	System Info	Hardware Version Active	0.0.9110
6	1.732 [008888C8]	IMEI	0 Active	3124768/8./902388.9
7	7.322 [00881C8F]	Security Code	0 Active	12.45
8	24.484 [00005FAE]	My Number	1 Active	0000000..00*.2
9	24.534 [00005FD6]	Mailbox Number	0 Active	671.2940
10	57.412 [0000E044]	ICC-ID and IMSI of Last SIMs	5 Active	894922200.1.15.5.00

Fig. 7: Excerpt of the CPA report for mobile phone information

1.2.6 Differences in the Operation Systems of Mobile Phones

We present the differences and particularities of currently used mobile phone operating systems within the following sections.

Nokia Series40

According to Nokia the Series40 platform has been developed over the last 8 years and the devices range from mass-market devices that provide many mobile consumers with their first experience of the Internet, to devices for specific market segments, such as music or fashion. This platform offers Java technology, Flash Lite from Adobe, web technology and mobile media content.

For Java developers, there is MIDP and CLDC technology, with an array of JSRs that provide additional location, communication, messaging, media and graphics capabilities. Media developers can deliver web, messaging and Flash Lite content, as well as streaming video and audio. All this is supported by Open Mobile Alliance (OMA) and digital rights management (DRM) to protect developers' property. OMA Client Provisioning (CP) and OMA Device Management (DM) to enable remote device configuration are also provided.

The device architecture, following to the Nokia white paper, consists of the hardware (the device hardware, CPU, memory) and the operating system, which provides fundamental services to the platform, which consists of:

- **Series40 applications:** functionality provided to the user, including communication applications (such as telephone and messaging), media applications (such as image viewer, camera and music player) and personal information manager (PIM) with calendar, tasks and contacts applications.
- **Series40 Java technology services:** the Java technology implemented within the platform.
- **User interface style:** resolution and input methods – a common set of UI components with defined behaviour used in one of a range of different screen orientations.

We provide a summary of the Java technology features supported by the different Series40 platforms in Fig. 8.

	Series40 1st Edition	Series 40 2nd Edition	Series 40 3rd Edition	Series 40 3rd Edition, Feature Pack 1	Series 40 3rd Edition, Feature Pack 2	Series 40 5th Edition	Series 40 5th Edition, Feature Pack 1	Series 40 6th Edition
CLDC support	1.0	1.1	1.1	1.1	1.1	1.1	1.1	1.1
MIDP support	1.0	2.0	2.0	2.0	2.0	2.1	2.1	2.1
Nokia UI API	X	X	X	X	X	X	X	X
PDA Optional Packages for the J2ME™ Platform (JSR-75)			PIM and FC packages	PIM and FC packages	PIM and FC packages	PIM and FC packages	PIM and FC packages	PIM and FC packages
Java™ APIs for Bluetooth (JSR-82)		v1.0, excluding OBEX	v1.0, excluding OBEX	v1.0, excluding OBEX	v1.0, excluding OBEX	v1.1	v1.1	v1.1
Wireless Messaging API (JSR-120)		X	X	X	X	X	X	X
Mobile Media API (JSR-135)		Sound playback	Sound, video, and image rendering	Sound, video, and image rendering	Sound, video, and image rendering	Sound, video, and image rendering	Sound, video, and image rendering	Sound, video, and image rendering
J2ME™ Web Services Specification (JSR-172)				XML parsing package	XML parsing package	X	X	X
Security and Trust Services API for J2ME™ (JSR-177)					SATSA-APDU package	SATSA-APDU and SATSA-CRYPTO packages	SATSA-APDU and SATSA-CRYPTO packages	SATSA-APDU and SATSA-CRYPTO packages
Location API for J2ME™ (JSR-179)								X
Mobile 3D Graphics API for J2ME™ (JSR-184)			X	X	X	X	X	X
Wireless Messaging API 2.0 (JSR-205)				X	X	X	X	X
Content Handler API (JSR-211)							X	X
Scalable 2D Vector Graphics API for J2ME™ (JSR-226)				X	X	X	X	X
Advanced Multimedia Supplements (JSR-234)						3D audio and music	3D audio and music	3D audio and music

Fig. 8: Summary of the Java technology supported by the Series40 platform

Symbian OS

Symbian OS has been created from scratch, especially for mobile communication devices. While other operating systems, e.g. WinCE for smart phones, had emanated from already existing operating systems, Symbian OS evolved from a contrary approach. The earlier version EPOC, for example, could be executed on devices with less than two megabyte of storage space.

Symbian supports not only different programming languages like Python and C++ and leads to a correlated significant increase in the availability of APIs, but moreover is build modularly. The operating system functionality is provided by the use of different components and not by a monolithic entity. Data access is executed by a 'file server' while user input and soft copies are displayed by the 'windows server', for instance.

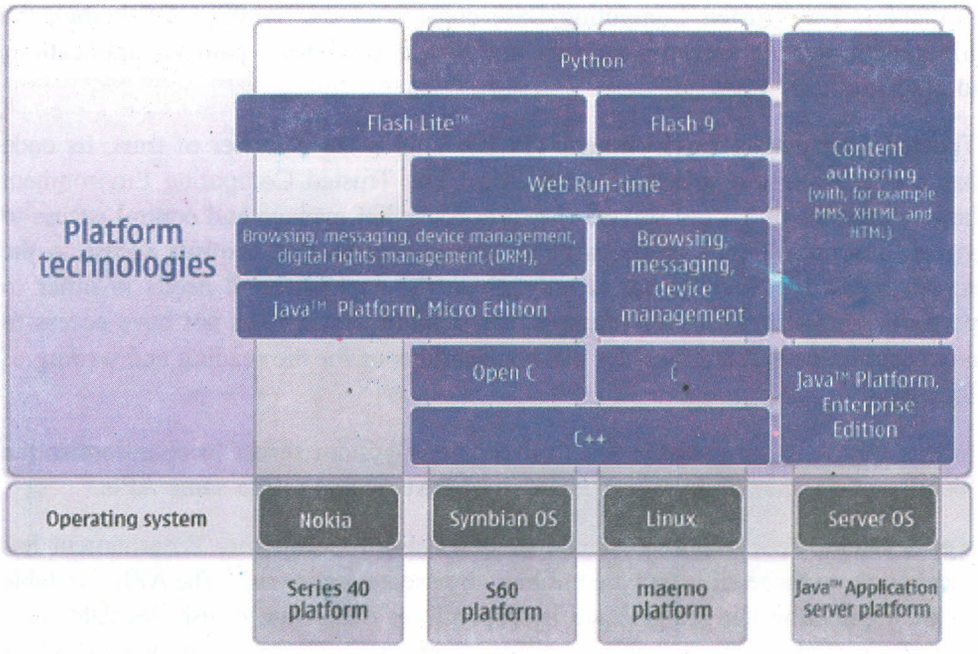


Fig. 9: Shows the differences of the Series40 and Symbian platform.

It is difficult to develop an operating system which possesses common core capabilities on the one hand and simultaneously features a uniform programming environment for all smart phones, on the other hand. Today's smart phones exist in different sizes, forms, screen sizes and input options. The user interface has to adapt to the respective conditions in order to cope with those requirements. Due to that reason Symbian is featured with a flexible architecture which allows the different user interfaces to use the core functionality of Symbian OS as a basis. With respect to mobile phone manufacturers, Symbian decided to develop some reference platforms as to give them a starting point. Those reference platforms include the Symbian OS core functionality together with a user interface which represents a basis-smartphone-type of a component assembly (screen size and input options). We state the two mostly used reference platforms in the following as an example:

Nokia S60: this also as Series60 known version already exists in the fourth version since 2001. Its key characteristics can be described as limited input options, a numerical keypad for text entry and a small screen size (typically 240 x 320 pixel).

UIQ: has been developed for pen-based (e.g. touch-screens) smartphones which is contrary to the S60. Mobile devices which are based on this platform often do not incorporate a keypad. However this disadvantage can be compensated by a virtual keypad and handwriting recognition. Screen size varies depending on the model

but it can be stated that 240 x 320 pixel are also typical for this type. An important point concerning Symbian is the Platform Security Architecture (PSA). It had been developed in order to control which operations a process is allowed to conduct and which not. A process can execute its function only if it owns the corresponding privileges. If a program does not own the necessary privileges, this process will be prevented from executing the operation due to the fact that it has been classified as untrustworthy.

The processes' access to APIs is administered by so-called 'capabilities'. Symbian OS constitutes a 'Trusted Computing Platform' which consists, according to Symbian, of three trust tiers:

Trusted Computing Base (TCB): This contains the most trusted parts of the OS. Its responsibility lies in the maintenance of the system's integrity and it is also the part that is least restricted (i.e. it has access to the full range of capabilities available). The Trusted Computing Base consists of the Symbian OS kernel, the file system and the software installer and how it provides a path for applications to enter the trust tiers.

Trusted Computing Environment (TCE): This is the next tier of trust. Its code has access to only a subset of capabilities. The Trusted Computing Environment largely consists of system servers (i.e. processes that manage and control access to system resources), such as the window server process that controls access to the screen hardware. Each server is only given the capabilities it needs in order to perform its function. So, for example, the window server does not have access to any capabilities that are used for communications or for the reading and writing of user data.

In this way it is not possible for a misbehaving system server to compromise the security of another server since it does not have access to the same APIs.

Application: Code running outside of the Trusted Computing Environment has access only to those APIs that are unlikely to pose a security risk. The APIs available in the application tier are grouped by capabilities that relate to user-level features or actions, that is, those that a user can understand. These capabilities are often known as 'user' capabilities or 'application' capabilities. Untrusted applications must request permission from the user before accessing these APIs.

The single capabilities of the correspondent trust tiers are shown in Fig. 10. With the help of signed software it is possible to add and/or modify components in the

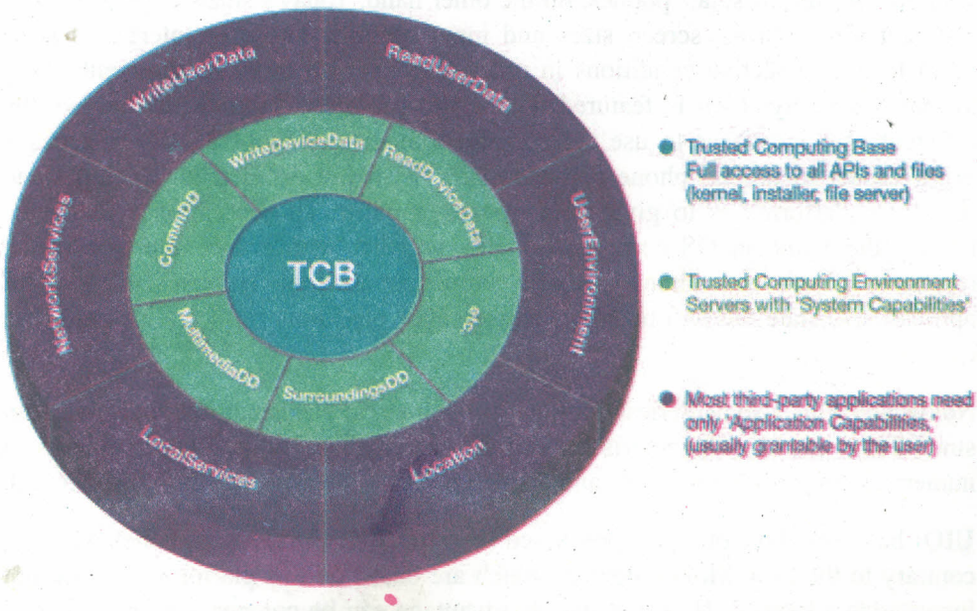


Fig. 10: The capabilities available in each trust tier

TCB or TCE. Anyhow, this holds only true if both, the software had been signed by a trustworthy certificate authority and the authority is qualified to grant the necessary privileges. A major implication of this is that signed software within the TCE is more trustworthy than software outside the TCE.

In case that either unsigned software is used or software which had not been signed by a trustworthy authority, the system has no basis on which the trustworthiness can be determined. This is why the software then is treated as not trustable.

Windows CE

Windows CE, often referred to as WinCE, is a modular operating system, which serves as the foundation for several classes of embedded devices. WinCE is optimized for devices with minimal storage and small scale factors. For example, its kernel requires less than 1 MB of memory. The devices are often configured without any disk storage and may be configured as closed systems, with the operating system burned on the ROM. WinCE are compliant to the definition of a real-time operating system with deterministic interrupt latency. It supports 256 priority levels and uses priority inheritance to deal with priority inversion. Furthermore, it is a multitasking operating system, where the fundamental unit of execution is a thread. Since the first edition of WinCE (Pegasus), the operating system has evolved to support platforms others than handheld devices.

To manage and allocate program memory, the WinCE kernel uses a paged virtual memory system. This system provides contiguous blocks of memory, between 1 KB and 4 KB within 64 KB regions, so that applications do not have to deal with memory allocation. In a WinCE device, the operating system and the applications bundled with the operating system, are stored in ROM. The entire operating system is mapped to a binary ROM image, logically divided into two types of modules. The first type corresponds to executable in place (XIP) modules.

The second type includes compressed modules, which are decompressed by the operating system and paged into RAM before execution. In WinCE devices, the RAM is divided into two regions, 'object store' and 'program memory'. The object store resembles a permanent, virtual RAM disk. Data in the object store is retained when the system is suspended or when a soft reset operation is performed. Normally, devices have a backup power supply for the RAM to preserve data when the main power supply is interrupted. When operations resume, the system searches for a previously-created object store in RAM and uses it.

The remaining portion of the RAM on a WinCE device is designated to program memory. This space holds various stacks and heaps belonging to executing applications. WinCE has a virtual memory address space of 4 GB. The operating system is able to manage at most 32 processes by assigning a slot corresponding to 32 MB of virtual address space to each process. This is partly due to the fact that Windows CE keeps the address spaces of all processes available at all times, even when the processes are not running. Thus, the lower portion of the address space is split into 32 MB slots. The address space is, according to Savoldi and Gubian, divided as followed:

- Slot 0 is assigned the memory locations in the range 0x00000000 to 0x01FFFFFF.
- Slot 1 is assigned the memory locations in the range 0x02000000 to 0x03FFFFFF.
- Slot 31 (last slot) ends at memory location 0x41FFFFFF.
- Memory locations in the range 0x42000000 to 0x7FFFFFFF mostly correspond to the 'shared area' used for VirtualAlloc functions and memory mapped files.

- Memory locations above 0x80000000 are reserved for the kernel. The kernel and the DLLs that load into the kernel execute from this memory space.

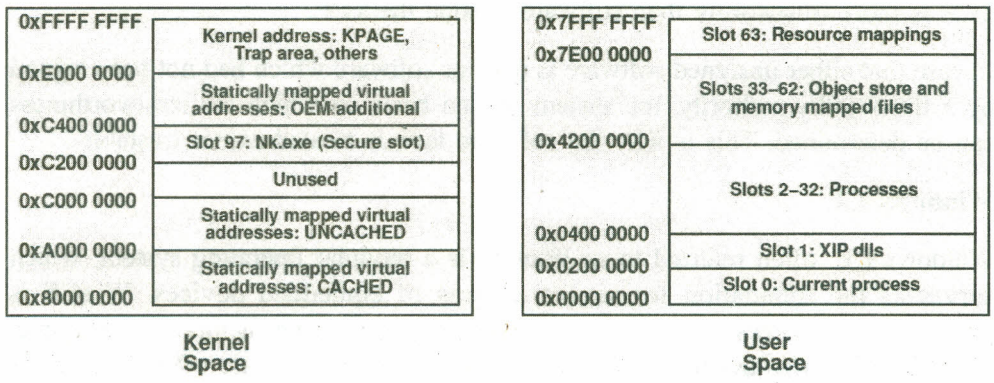


Fig. 11: Virtual address space managed by Windows CE

Fig. 11 shows the layout of the virtual memory managed by WinCE. Note that the kernel and user space each have 2 GB of addressable memory. The Remote Application Program Interface (RAPI) protocol is often used by tools to extract the ROM and RAM contents of WinCE devices. The RAPI library enables applications running on a desktop computer to perform actions on a remote WinCE device. RAPI interfaces can be used to create and modify databases, either in the object store or in mounted database volumes. RAPI applications can also query and modify registry keys as well as launch applications and invoke methods on the remote device.

OS X iPhone

The iPhone has a solid state NAND flash included which is divided into two partitions by default. The root partition has, depending on the iPhone's generation, a size of 300MB up to 500MB and contains pre-installed software which is intended to remain on the phone over its complete lifetime. Due to that reason the partition has a read-only status and is directly mounted under /. The residual storage space is mounted as a media partition under /private/var/ and serves for the storage of all user data including music, contacts and pictures.

According to Zdziarski this exhibits the best possibility for Apple to load a new operating system onto the phone without changing any user data. The actual device nodes for the disk are as seen in below Listing.

```
brw??r?????? 1 root operator 14, 0 Apr 7 07:46 /dev/ di sk0 Di sk
brw??r?????? 1 root operator 14, 1 Apr 7 07:46 /dev/ di sk0s1 System
brw??r?????? 1 root operator 14, 2 Apr 7 07:46 /dev/ di sk0s2 Media
```

Listing : Device nodes for iPhone disks

Both partitions make use of the by Apple developed HFSX file system which is shown together with the partition type (pmParType) 'Apple HFSX'. The above mentioned file system constitutes an advancement of HFS+ which is case sensitive when dealing with file names and which has activated the journaling function of HFSJ by default. According to Apple case-sensitive names do not ignore Unicode 'ignorable' characters. This means that a single directory may have several names which would be considered equivalent using Unicode comparison rules, but which are considered distinct on a case-sensitive HFSX volume. Those volumes can be identified by the signature 0x4858 in the signature field of the volume header. The following version field specifies the in the volume used HFSX-version7.

HFS+ is a 32-bit file system with an universal Unicode character set and an up to 255 characters long file name. It is able to administer up to four billions of blocks which may contain files and/or folders. This is not only dependent on the size of the medium used, but also on the files and the blocks itself. The preferable block size is 4 KB.

1.3 MOBILE FORENSIC TOOLS

Data can be retrieved from a mobile device by using forensic software and being able to connect to the mobile device either by a cable, Bluetooth or an infrared connection. Examples of such software are Oxygen Forensic Suite, SIMIS and data doctor phone inspector. One type of software may produce a more detailed and precise report in a specific area but may lack detail in another. Another method a forensic analyst could use is to access information directly from the mobile by the use of the keypad if possible but this is a risky method and should be used as a last resort as there is a high chance of data being modified if a wrong button is pressed. The number one objective is to extract as much data as possible without altering any data in the process. The analyst must also be careful not to lose any information e.g. some phones store data on missed and received calls on the SIM card.

Another factor that must be addressed when carrying out a forensic analysis on a mobile phone is to keep it out of electromagnetic contact as even in an idle state a mobile is constantly trying to communicate with a network. What may happen is new data is sent to the mobile that may overwrite existing data for example this new contact with the network could have destroyed potential evidence such as a SMS message or a missed call. It is very important that no data is manipulated during the process of removing data if the data is to be used as evidence. So during a procedure to extract data from a mobile phone to a computer a log file is created which records all communication between the computer and the phone so that it can be satisfactorily demonstrated that no data has been written to the phone during the extraction process. Some of the important pieces of evidence for forensics are the address book which can contain various types of data from numbers to pictures and the call history of the phone as well as the message history and other forms of media that is stored on the phone. Much of these items can be retrieved with little need for sophisticated tools, however, when it comes to the other identifying items such as deleted contacts and erased history - then dedicated software is needed. Many of the leading forensics tools are usually licensed from specialists that have developed their own bespoke version of forensic software. Forensic software will retrieve the information from the phone either by targeting a physical aspect of the phone or a logical aspect. A physical aspect of a mobile would be the SIM as this is an independent storage device and can be separated from the phone, as well as possibly a memory card such as a MicroSD card. A logical aspect is the directories or files residing on the phone. Both physical and logical aspects are key areas for forensic investigation. When deciding what type of software to use, it is also important to take into consideration the type of network the phone is on as well as the actual software OS. There are different types of software some specializing for instance on smart phones and others on Symbian devices.

The software applications for mobile forensics available today are not 100% forensically sound. The reason is that they use command and response protocols that provide indirect access to memory. This means that the forensic software does not have direct access or low level access to data within the phone's memory as it depends on the mobile phone's operating system based command to retrieve data in the memory. Therefore in querying the operating system, the device could be creating changes to the memory of the device. Some command based mobile

forensics software was not originally developed for forensic purposes and therefore they could unexpectedly write to the mobile phone device's memory. Sometimes forensic software such as MOBLedit Forensic1 requires the user to install additional software on the mobile phone being examined.

There are alternative methods to gain direct access to data held on mobile phones which do not breach best practice guidelines. Flasher boxes for instance can provide this direct access to data held on mobile phones without the need of resorting to operating system software or hardware command and response protocols. Flashers are a combination of software, hardware and drivers. Flasher boxes do not require any software to be installed on the mobile being examined. In theory, this should ensure that they do not manipulate any data that may be used as evidence.

However, because they are not usually documented, there are no easy methods of determining if they do actually preserve evidence in the phones memory and there is no guarantee that the flashers will work in a consistent manner. It must be noted that mobile phone companies have not approved or tested flasher boxes on their products nor have they been tested or approved for forensic use.

The Cellebrite UFED System2 (Universal Forensic Extraction Device) is a mobile hardware device which accepts SIM cards. It will also allow access to the phonebook, text messages, call history (received, dialed, missed), deleted text messages from SIM/USIM, audio recordings, video, pictures and images and more.

PDA Seizure3 facilitates accessing information on a PALM or Blackberry PDA. It also allows the retrieval of information on the physical and logical parts of the PDA device. This software is windows based. Device Seizure is similar to PDA seizure but more comprehensive in provided features. It allows deleted data recovery, full data dumps of certain cell phone models, logical and physical acquisitions of PDAs, data cable access and advanced reporting. It provides access to phones via IrDA and Bluetooth.

Some approaches rely on the AT command system developed in the late 1970s to initialize modems to ask the phone specific questions about the information it may be storing. However, not all mobiles respond to modem-style commands with for instance Nokia phones being particularly hard to crack.

The initial preservation stage should secure the evidence and to record and document in its current state so as to prevent tampering with the evidence. Documents for the scene including photographs of the phone undisturbed should be included. When handling and moving the device one point is to keep it away from harmful elements such as high temperatures and any large magnetic sources that may affect the device. There also needs to be great care taken to preserve the DNA evidence that could be on the phone including finger prints or saliva. All accessories for the phone should be acquired if possible and taken as part of the evidence for testing. Another aspect of preservation is to note whether or not the phone was on when found, for this reason the phone should be turned off so as to stop any further interaction with radio waves that may cause some data on the phone to overwritten. The acquisition stage is where a copy of the data from the phone is made. This should be a mirror image of the SIM data and relevant memory cards. This process will usually happen in a lab however there can be problems due to battery damage or excess damage to the phone. This stage is when forensic tools are used most. Currently there is no one tool that can be used on all phones so there would be a range of software used in order to acquire the data. Here it may be common to encounter problems when trying to acquire the data through items such as pin protection. Fortunately, contacting the network providers can solve many of these problems as many networks will have a backdoor way to access the data on the device. The analysis stage is where the data is examined. This part of the process needs to be done carefully so as not to miss anything that

may be relevant to the case. The examiner ideally should be familiar with the work that has gone on prior to the examination. Finally, the reporting stage is where the evidence is summarized so as to be presented in court as evidence.

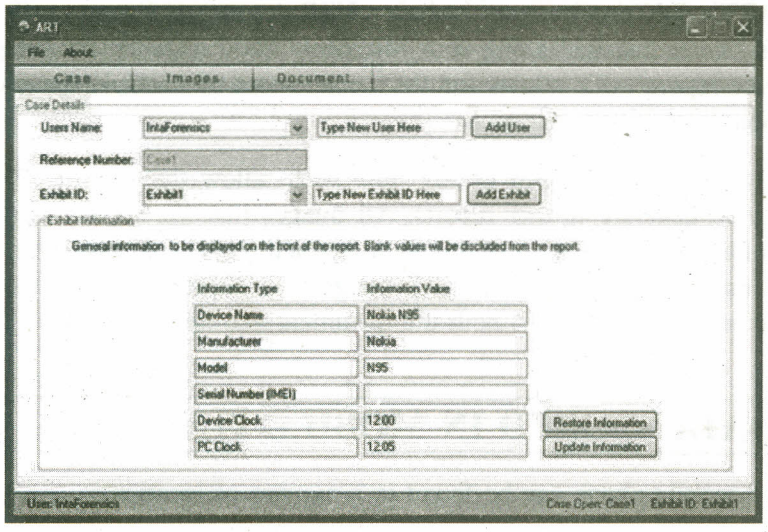


Fig. 12: Information on each exhibit in ART

A number of companies provide the service of mobile phone forensic analysis. These include Inta Forensics, Mobile Phone Forensics, Integrity Forensics, Sector Forensics and CY4OR. Whilst all these companies offer a similar services and follow similar analysis techniques different report application software is used to present the retrieved data.

As with many of the other mobile phone forensic analysis providers, Inta Forensics uses their own in house software application called ART (Automatic Report Tool) (see Fig. 12). This application allows mobile phone forensic examiners to capture images (via a camera) of mobile devices and subsequently produce a Microsoft Word document. ART is supplied by www.IntaForensics.com for free to registered users conducting Mobile Phone Forensic Analysis.

Whilst all these companies offer a similar services and follow similar analysis techniques different report application software is used to present the retrieved data.

As with many of the other mobile phone forensic analysis providers, Inta Forensics uses their own in house software application called ART (Automatic Report Tool) (see Fig. 13). This application allows mobile phone forensic examiners to capture images (via a camera) of mobile devices and subsequently produce a Microsoft Word document. ART is supplied by www.IntaForensics.com for free to registered users conducting Mobile Phone Forensic Analysis.

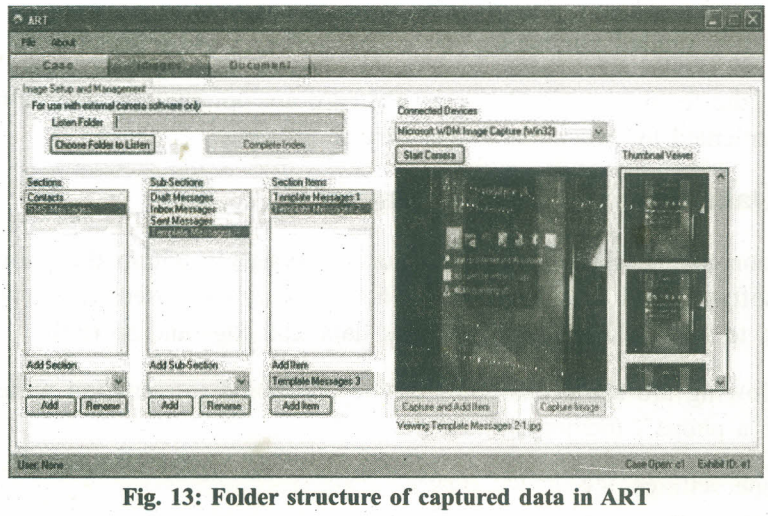


Fig. 13: Folder structure of captured data in ART

The main benefits of using ART is that it allows its users to capture images from USB camera and then store these images under appropriately named folders and then publish a customizable report containing the captured images of the mobile device. ART's only requirements include a USB or external Camera with Microsoft Windows Driver installed along with Microsoft Word installed for the generation of a device report. ART allows for the management of multiple cases containing large amounts of visual evidence.

These cases can be accessed at any time so to allow the capture of additional images or to generate further reports. All images that are captured are saved to folders reflecting the location of the photographed object for easy reference by the user and easy report generation. ART design also allows for basic formatting of the report prior to printing in both the document and header sections.

1.4 DATA STORED IN MOBILE PHONES

Data on a mobile phone can be found in a number of locations:

- The SIM card (if present).
- The phone's embedded memory.
- The phone's removable memory (i.e. SD card), if present.

In addition to this, subscriber and call related information is also stored by the service provider.

1.4.1 Data Stored in SIM Card

The Subscriber Identity Module or SIM card, used in GSM phones, is a smart card which enables connection to GSM networks and enables the subscriber to be uniquely identified in the network. The SIM card contains a number of files, which contain the user's subscriber information and personal information, such as:

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

Many of the features available on a SIM card are optional and therefore may not be implemented by every handset or service provider.

1.4.2 Data Stored in Phone Memory

In addition to the SIM memory, memory is available within the phone to store phone software and additional data. This space can be used to extend the SIM memory, to store 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:

- Phone settings

- Calendar information
- SMS/MMS messages
- Call log entries
- Time and date
- Ring tones
- Data required for/produced by the phone's extra features, such as audio and video recordings and images
- Generic data stored in the phone's memory
- Application executables.

Many modern phones come with a relatively large amount of onboard memory. For example, the Nokia 9300 has 80MB onboard memory, with the option to extend it with a removable memory card (Nokia 2005b).

These removable cards are generally used to store multi-media files, such as audio, video, images and MMS messages and are not used for phone related information (phone book entries, etc). However, the cards can be used for transfer and storage of any form of data.

OBEX capable phones will typically allow the user to store any form of data in the phone's memory. While the phone may not be able to recognise or display the data, it can be used as a generic storage device.

1.4.3 Data Stored by the Service Provider

Data retained by the service provider includes subscriber information, location information and call and billing information. Whenever a call is made or a text message is sent, a 'call data record' is created and stored, containing, amongst other information, the sending and receiving phone numbers, the length of the call and the initial and final location of the two parties. This information is available from the service provider and therefore is not discussed as it is outside the scope of this thesis.

1.5 EXTRACTING DATA FROM MOBILE PHONES

It is important to realise that there are a number of basic requirements for a handset and/or SIM card to interface with a computer. Once these requirements are met, the manufacturer is free to implement any other features in any way it wishes. This means that a forensic tool for mobile phones will not be able to target every feature on every type of phone.

Furthermore, the different technologies upon which mobile networks are based, such as TDMA, CDMA and more recent 3G technologies, such as WCDMA, each require the handsets to implement different standards. For example, CDMA phones do not require a SIM card; rather, the software required to connect to the network is in the phone itself.

Data will either be found in the SIM card if present or in the phone's memory.

There are a number of different methods for obtaining the data. However, there is no accepted standard, as the freedom which manufacturers have when designing their phones means that every phone must be considered separately.

The following methodology is generally proposed for forensic analysis of phones:

- Turn the phone off as soon as possible.
- Obtain access codes from the phone owner / service provider
- Analyse the SIM card.
- Analyse any removable memory.
- Analyse the phone memory.

This methodology raises some issues. The importance of isolating the phone from the network, so no new information is received is required to be stated. Turning the phone off has the potential to alter data on the phone, but leaving the phone on raises the possibility of new information arriving over the network.

There are ways around this issue; for example, Forensic Telecommunications Services offers a 'radio screened foil bag' which isolates the phone from the network. In the absence of such equipment, turning the phone off should be the preferred choice; however, a certain level of trust must be placed in the phone's operating system. It is also be noted that the order in which data is extracted is important, as removal of the SIM card or battery from some phones will modify the contents of the phone memory. This raises the question of whether the SIM card should be removed from the phone before analysis/imaging. Many phones require the battery to be removed to access the SIM card. This has the potential to alter information in the phone. An example of this with regards to the Nokia 3310 handset, which loses time and date information as soon as the battery is removed.

Removing or replacing the SIM card may also have an effect on the phone's memory and it is to be noted that another method of obtaining data from both the phone and the SIM card is to simply use the phone's keypad to browse through the phone. However, certain information such as deleted text messages would not be accessible via this method and the process is time consuming and prone to errors, as pushing the wrong keys could destroy information.

Phone and SIM access codes will generally be needed before certain information can be accessed. These will either be obtainable from the phone's owner (PIN codes) and/or the service provider (PUK codes).

1.6 EXTRACTING DATA FROM SIM CARDS

Forensically acceptable extraction of data from the SIM card can potentially be accomplished in two ways. Directly analysing the contents of the SIM card is outside of the scope of this thesis and hence will not be discussed in a detailed manner.

The first way is through a smart card reader, which are cheap and easy to obtain. The SIM card is accessed and controlled by commands specified in the ETSI 'TS 31.101' and 'TS 51.011' standards (ETSI 2000, 2004). A terminal program such as Microsoft HyperTerminal can be used to send commands to the SIM card. A number of software applications are also available which perform these tasks, such as SIM Manager and SIMCon.

Another method of accessing the SIM card is through the mobile phone. GSM phones conform to the ETSI 'TS 27.007' standard, which specifies a command set. This set includes a command which allows a SIM card command to be embedded and passed to the SIM card. Responses from the SIM card are passed back in a similar manner. This is effectively identical to directly accessing the SIM card. This command is an optional implementation, however, so there is no guarantee that every GSM phone supports it. If this method were available on

every mobile phone, it would reduce the difficulty in analysis, as the SIM card would not need to be removed and analysed separately.

1.7 EXTRACTING DATA FROM PHONE MEMORY

The data to be extracted will reside in the phone's embedded memory and / or in a removable memory card. Data stored in the latter is examinable using a forensic tool such as Encase. Extracting data from the phone's embedded memory is more complex. Two forensically sound methods are proposed:

- Taking the phone apart and accessing the memory chip directly.
- Tapping in to the phone's motherboard to access the memory chip.

These two methods bypass the phone's operating system and access the memory directly; hence, an exact memory image can be obtained. The only way to directly access the phone's memory is through one of these methods.

The use of the JTAG interface may also allow a complete memory image to be obtained in a non-destructive manner. Due to their technical nature however, it is currently infeasible to expect the average investigator to use these or any similar methods.

Therefore, an exact image of a phone's memory cannot be obtained by a non - technical investigator. The methods described above are infeasible, as they would involve detailed knowledge of the phone's design. Thus, the only acceptable method of data extraction is through the phone's software interface. However, analysis using this method places trust in the phone software, that it does not alter the phone's memory. This trust problem is confirmed by who also notes related issues, namely that deleted information will not be accessible via a software interface.

Best practice guidelines from the 2000 International Organization on Computer Evidence conference (IOCE 2000) state that phones and other electronic devices should be examined with 'methods that minimise loss / change of data'. It is simply too much trouble to obtain an exact memory image. Therefore, the phone's (and SIM card's) operating system must be trusted not to alter the memory when read commands are executed.

1.8 MANUFACTURER AND THIRD PARTY SOFTWARE

Software packages for data synchronisation between phone and computer are generally available from the phone manufacturers. The phone is usually connected via a data cable or by infra-red or Bluetooth. Some examples of such software are:

- Nokia PC Suite (Nokia 2005c).
- Sony Ericsson Sync Station (Sony Ericsson 2005a).
- Sony Ericsson File Manager (Sony Ericsson 2005b).

Third party software which performs the same function is also available, such as MightyPhone. These applications are not designed for forensic analysis; hence there is a risk in altering the data on the phone through improper use of such an application.

Nokia PC Suite and Sony Ericsson Sync Station were reviewed using a freeware serial port monitor, Portmon and a USB monitor, SourceUSB. This review was performed to determine the methods these applications use to communicate with

the phones. It should be noted that wherever communication between a mobile phone and a PC has been referred to, the assumption has been made that the output from these monitor applications reflects the communication which is actually taking place.

Nokia PC Suite was tested with a Nokia 3220 and Nokia 6225, using an official Nokia CA-42 USB cable. There are a number of different versions of the software, however in this case, the same version was recommended for both phones. Predictably, the software uses Nokia's proprietary FBUS protocol for all communication with the phones and is able to extract the phone book, call logs and calendar entries. OBEX is used to extract media files, ringtones and downloaded applications. PC Suite could extract SMS messages from the 3220, but not from the 6225.

Sony Ericsson Sync Station and File Manager were tested with a Sony Ericsson f500i using an official Sony Ericsson DRS-11 serial cable. Sync Station is an application used for synchronizing the contents of the phone with an application such as Microsoft Outlook. Data such as contacts and calendar entries can be copied between the phone and an application to ensure both data sets are identical. Sync Station used SyncML over OBEX to extract the phonebook and calendar entries from the phone.

Sony Ericsson File Manager is an application which allows a limited portion of the phone's file system to be accessed. The application used OBEX to access user created/downloaded media files. Only a subset of the phone's file system was accessible.

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

How data can be extracted from phone memory?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

1.9 LET US SUM UP

This unit deals with the "Introduction to mobile forensics and technologies". We covered Mobile Forensic Tools and data stored in Mobile phones in detail. We discussed Extracting data from Mobile phones, from SIM Cards and from phone memory.

1.10 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

Extracting data from phone memory

The data to be extracted will reside in the phone's embedded memory and/or in a removable memory card. Data stored in the latter is examinable using a forensic tool such as Encase. Extracting data from the phone's embedded memory is more complex. Two forensically sound methods are proposed:

- Taking the phone apart and accessing the memory chip directly.
- Tapping in to the phone's motherboard to access the memory chip.

These two methods bypass the phone's operating system and access the memory directly; hence, an exact memory image can be obtained. The only way to directly access the phone's memory is through one of these methods.

The use of the JTAG interface may also allow a complete memory image to be obtained in a non-destructive manner. Due to their technical nature however, it is currently infeasible to expect the average investigator to use these or any similar methods.

Therefore, an exact image of a phone's memory cannot be obtained by a non - technical investigator. The methods described above are infeasible, as they would involve detailed knowledge of the phone's design. Thus, the only acceptable method of data extraction is through the phone's software interface. However, analysis using this method places trust in the phone software, that it does not alter the phone's memory. This trust problem is confirmed by who also notes related issues, namely that deleted information will not be accessible via a software interface.

Best practice guidelines from the 2000 International Organization on Computer Evidence conference (IOCE 2000) state that phones and other electronic devices should be examined with 'methods that minimise loss/change of data'. It is simply too much trouble to obtain an exact memory image. Therefore, the phone's (and SIM card's) operating system must be trusted not to alter the memory when read commands are executed.

UNIT 2 ANALYSIS OF CDR'S

Structure

2.0 INTRODUCTION

For every mobile telephone call there should be a corresponding Call Detail Record (CDR). It can contain information that the mobile network operator uses for subscriber identification, call charging, services obtained, call routing etc.

2.1 OBJECTIVES

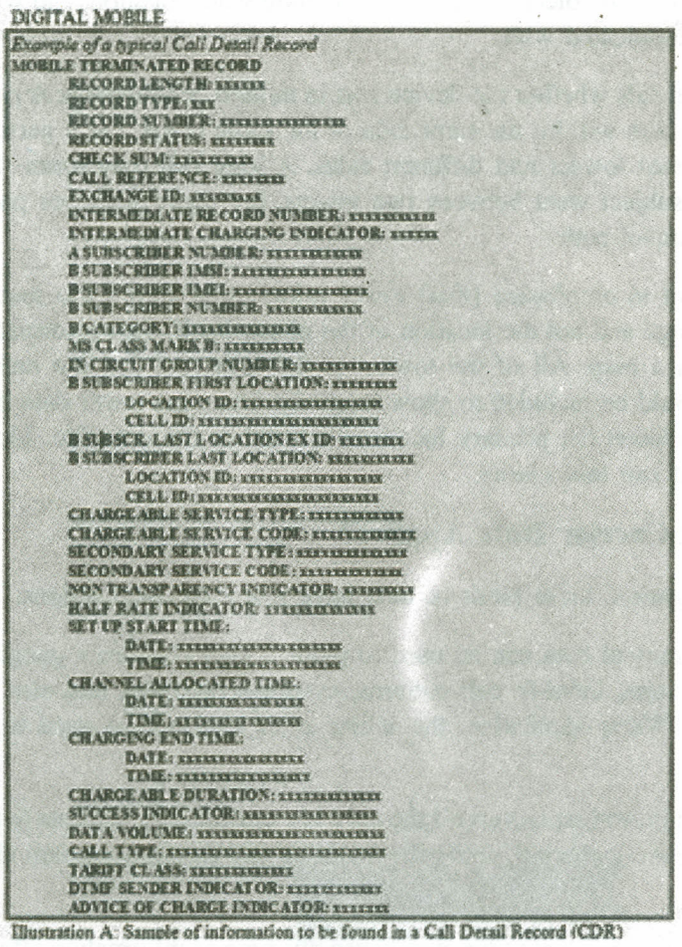
After going through this Unit, you should be able to:

- understand and explain about Call Detail Records (CDR's);
- list types of call data; and
- explain analysis of CDR's.

2.2 CALL DETAIL RECORD (CDR)

A Call Detail Record (CDR) can contain the identification of the start and end cell. Do remember, for the purposes of accuracy, a Call Detail Record is a single record of a mobile telephone call and is legally and Standards recognised. The mobile terminated call (MTC) CDR example is included in my work that I was commissioned to prepare and published for Dr Bainbridge Aston University: Admissibility of Computer Evidence in Criminal Proceedings, 1998. The relevance

of mentioning this is that there is nothing new about cell identification being recorded in a Call Detail Record.


DIGITAL MOBILE

Example of a typical Call Detail Record

MOBILE TERMINATED RECORD
- RECORD LENGTH:
- RECORD TYPE:
- RECORD NUMBER:
- RECORD STATUS:
- CHECK SUM:
- CALL REFERENCE:
- EXCHANGE ID:
- INTERMEDIATE RECORD NUMBER:
- INTERMEDIATE CHARGING INDICATOR:
- A SUBSCRIBER NUMBER:
- B SUBSCRIBER IMSI:
- B SUBSCRIBER IMEI:
- B SUBSCRIBER NUMBER:
- B CATEGORY:
- MS CLASS MARK B:
- IN CIRCUIT GROUP NUMBER:
- B SUBSCRIBER FIRST LOCATION:
  - LOCATION ID:
  - CELL ID:
- B SUBSCR. LAST LOCATION EX ID:
- B SUBSCRIBER LAST LOCATION:
  - LOCATION ID:
  - CELL ID:
- CHARGEABLE SERVICE TYPE:
- CHARGEABLE SERVICE CODE:
- SECONDARY SERVICE TYPE:
- SECONDARY SERVICE CODE:
- NON TRANSPARENCY INDICATOR:
- HALF RATE INDICATOR:
- SET UP START TIME:
  - DATE:
  - TIME:
- CHANNEL ALLOCATED TIME:
  - DATE:
  - TIME:
- CHARGING END TIME:
  - DATE:
  - TIME:
- CHARGEABLE DURATION:
- SUCCESS INDICATOR:
- DATA VOLUME:
- CALL TYPE:
- TARIFF CLASS:
- DTMF SENDER INDICATOR:
- ADVICE OF CHARGE INDICATOR:

Illustration A: Sample of information to be found in a Call Detail Record (CDR)

Fig. 1: Sample Call Detail Record of GSM

The above is one example of the core-skills content available through my training courses and I have posted this information because I have heard from and read comments from those who have attended other providers' training courses who have received what is said to be forensic and expert training for the purposes of providing mobile telephone evidence and services and which the comments imply or infer that the training turns out to be partly or entirely unsuitable to deal with the understanding of the subject matter. This is leaving those who attended those training courses to vulnerability when examining, investigating or providing opinion about mobile telephone evidence.

A cell phone isn't just a surface from which to lift a fingerprint, a device that reveals known associates or even a repository of messages and images. There's another side to mobile forensics: service provider (or carrier) data, including call logs, undelivered messages and tower data – data that shows a cell user's location at the time of an incident. Matched with the information saved to the device and mapped together with street names and landmarks, carrier data supplements and enhances device data. It can even break a case. Yet too often investigators overlook this critical evidence.

2.2.1 Carrier Data: An Evidence Cornerstone

Most cell towers consist of poles that send and receive signals in three sectors: alpha (north-facing), beta (southeast) and gamma (southwest). This configuration makes it easier for carriers to improve service by covering an entire hexagonal "cell" within the network. It also enables them to identify which sector of the antenna (which side of the tower) communicated with a cellular device.

Carriers keep detailed call records of these communications for billing purposes, so the data includes information like date, call length, whether a call was inbound, outbound or went to voicemail; the tower's number and location; and which antenna the call communicated with.

Tower data reveals whether the device was in motion or stationary. A person dialing from one location will hit the same side of the same tower, but a person on the go will hit different towers and different sides. A long call may make it difficult to tell where a subject went between two towers, but short messages paint a clearer picture of a travel path.

It is important to emphasize [that] tower information shows the sequence of the cell tower usage and not the location of the phone itself. This information is easily visualized on a map. All of the towers in the area (not just the ones the phone accessed) should be included to show relativity. Once the tower data is completed, one needs to insert the primary locations notated in the case file. More than that the map itself can lose clarity.

2.2.2 How Carrier Data Applies?

In an investigation, these kinds of data have important implications.

Primarily, historical data can be used to place a phone within a geographical area at a specific time, identify call patterns, establish timelines and also identify co-conspirators. When applicable, the information also can be used to corroborate statements.

After-the-fact investigations aren't the only law enforcement aspects to utilize tower data, intelligence-gathering, anti-gang, narcotic and counterterrorism units can also benefit.

One misconception is that you can only use this type of information after an incident has occurred. The fact is, if you have a suspect that you believe is involved in criminal activity and you would like to know where he was one week ago, you can contact the carrier to obtain that information without having to have any contact with the suspect. All you need is the suspect's cell phone number.

Tower data also comes into play during missing-persons searches. As one case, the investigators had put a helicopter over the tower on the side that showed the last hit. Even though both passengers were deceased, to find the plane within 20 or 25 minutes instead of hours or even days worked to everyone's benefit.

As cell phone technology advances, the devices are frequently linked to unconventional crimes that test both existing statutes and legal precedents. Vehicular homicide, for example, virtually demands that a suspect's cell phone be seized and the call logs, SMS messages with their date/time stamps, etc. be preserved. This way, investigators can determine whether cell use, including "driving while texting", was a factor.

2.2.3 Carrier Data Challenges

While customer demand for better coverage – and thus more towers – remains high, Loving says many communities have limited tower build-out for a variety of reasons, including aesthetics, zoning and site problems and even public health. That's why many carriers have begun to share tower space.

It is not uncommon to find two or three different carriers at one location. The simplest and fastest way to determine if multiple carriers exist at one location is to view the tower location. You will notice a group of antennae on the tower; and individual, bulletproof control rooms/buildings at the base.

This is important for investigators to know because collectible data doesn't go by tower; it goes by carrier. Each carrier maintains sets of information for different periods of time, ranging from six years to just 45 days for call detail reports, while text messages and voicemail typically last a week or less. Each carrier also has its own preferences for how it wants to receive and deal with subpoenas. Some may even charge money for records retrieval services.

Some time even personnel changes can create difficulties. Investigators may have had limited or no prior contact with service providers and have no idea where to start. They may not know what information is available to them or what the company's data preservation timeframe is.

These factors can lead investigators to assume erroneously that they'll have a hard time getting a warrant. But the trick isn't obtaining the warrant; it's doing so quickly enough.

The best way to accomplish this is to send a preservation letter. Such a letter asks carriers to pull and maintain data until a warrant can be obtained.

2.2.4 The Carrier Data/device Relationship

That one set of evidence cannot exist independently of the other during a criminal investigation, for a variety of reasons.

First, no standards exist for cell phones. The fact that different carriers utilize different technologies and have more than 100 different handsets on the market at any given time [makes] evidence collection/data recovery extremely challenging.

Manufacturers are unlikely to ever standardize their equipment. To stay competitive, they cannot standardize things like memory and connectors and they are constantly improving the technology for faster data and better storage. So whereas a computer's hard drive is static and easy to image, investigators would have to budget thousands of dollars in software upgrades alone to keep up with cell device manufacturers. Hence, the need to work with carriers to obtain data.

Conversely, tower data tells only part of the story. One challenge law enforcement faces is identifying the specific user of a phone. The only way to positively identify a user is through personal statement, direct observation or audio identification.

For example, after a murder tower data that showed the suspect fleeing the area was later tied to personal data in his phone's calendar. That tower data showed calls being made along the suspect's escape route; the suspect had even erased all inbound and outbound call logs.

The relationship between device and carrier data is even more intertwined when it comes to SMS (text) messages. Encoded using Protocol Description Unit (PDU) mode, a GSM standard, the SMS message contains much more than the message: it also includes "metadata," information on the phone number dialled, the date and time the message hit the service center and the center's phone number. This data, which users can't view, is important to law enforcement. The carrier maintains the information that will help law enforcement identify the subscriber.

As technology evolves it presents more to investigate.

Evidence locations can be broken down into four parts:

- Service providers. "Airtel, Vodafone, Aircel, MTNL [etc.] all have different internal systems that collect, maintain and provide data in different ways from each other.
- Networks. As noted, providers sometimes share networks via tower antennas.

- **Mobile forensics:** Not only does it identify what carrier the device works on it also reveals current and potentially deleted photos, text messages, call logs, voice and video recordings and other evidence.
- **Phone manufacturers:** This comes into play when you find phones with the same capabilities, but [with] different software, since it works on a different carrier's system.

In addition to device and carrier data, cell phones may provide access to other important information. A GPS-enabled device will have data logs associated with it, either from the cell carrier or from the third-party GPS carrier whose software has been downloaded to the phone.

The phone's registration will contain credit information and other applicable data. Even a prepaid phone requires registration. Although a user can sign up as Mickey Mouse, personal information will be available.

It's important to record equipment identifiers, including the electronic serial number (ESN), the International Mobile Equipment Identity (IMEI) number, the handset model number itself and removable media such as Flash cards. Information on a SIM is standardized by ETSI [the European Telecommunications Standards Institute] and 3GPP [3rd Generation Partnership Project]. It is really the handset, the manufacturers and carriers who have different firmware that allocate different portions of storage areas for data, which are not necessarily standardized.

2.2.5 Pulling it All Together

Mobile forensics is becoming increasingly complicated to navigate, even as it becomes more important in criminal investigations. Law enforcement agencies should thus ensure proper training for their personnel. In the last two years, there has been an increase in the number of departments putting officers through courses.

Training is also important for first responders, who must know how to preserve both the phone and the evidence inside. It's not enough to seize the cell phone during an arrest; the officer must also immediately ensure that its data remains intact. An arrested person can use his one phone call to contact an associate, who can then log on to the carrier's Web site and delete information. If the phone is on or turned on during an investigation, the data will be deleted as soon as it connects to the network.

Some investigators prefer to use a "Faraday cage," a signal disruption device that allows the phone to turn on without it connecting to the network. (Digital forensic solutions provider Paraben Corp. has designed a Faraday evidence bag that first responders can use to secure mobile devices.) It is also recommended turning on the seized phone's "flight mode" feature, which enables the device's full functionality without a network connection.

The carriers themselves supply the other part of a solid investigation. Today, most companies have a department assigned to handle law enforcement requests and maintain the level of confidentiality that investigations require.

This represents a major change from even a few years ago. The telecommunication business was designed to be consumer-driven, not a source of potential evidence used in the courts. Additionally, the companies are required to protect their subscribers' privacy. Balancing the two requires personnel to assure legal compliance, as well as answer law enforcement questions, process requests and, when necessary, provide expert testimony.

2.3 TYPES OF CALL DATA

Cell phones are highly mobile communications devices that can do an array of functions ranging from that of a simple digital organizer to that of a low-end personal computer. Designed for mobility, they are compact in size, battery powered and lightweight, often use proprietary interfaces or operating systems and may have unique hardware characteristics for product differentiation. Overall, they can be classified as basic phones that are primarily simple voice and messaging communication devices; advanced phones that offer additional capabilities and services for multimedia; and smart phones or high-end phones that merge the capabilities of an advanced phone with those of a PDA (Personal Digital Assistant).

Using the latest advancements in digital technology, one can develop the capacity to provide a comprehensive mobile phone forensic analysis.

CDR analysis is basically retrieval of all forms of data stored on mobile phone devices including SIM card data recovery, test and SMS data recovery, picture recovery and call log recovery. Of the mobile phone data recovered Forensic Resources can retrieve phone book contact numbers from the SIM card including SIM Card contacts locked with a PIN or without the original SIM.

In short the following data require being retrieved and analyzed:

- SIM Card Analysis
- SIM Card Data Retrieval
- Picture retrieval from mobile phone devices
- Phone book data retrieval
- Call log recovery and call log analysis
- Text message and SMS message recovery
- Call Pattern Analysis
- Usage profiles
- Forensic Analysis of billing records
- Forensic Analysis of mobile phone downloads
- Forensic Mobile Phones Analysis

2.4 SIM CARD ANALYSIS

Subscriber Identity Modules (SIMs) are a fundamental standardized component of most cell phones used worldwide. A SIM can be removed from a phone handset and inserted into another, allowing users to port identity, personal information and service between devices. All cell phones are expected to incorporate some type of identity module eventually, in part, because of this useful property.

Some of the earliest, general purpose, forensic tools for cell phones targeted SIMs to recover digital evidence. While over time the capabilities and number of such tools have increased, they are not completely free of problems. Validating a forensic SIM tool is an essential quality assurance measure. It allows a forensic specialist to determine how to compensate for any shortcomings identified or whether to use one version of the tool in lieu of another. Tool manufacturers also benefit from rigorously validating their products before releasing them. However, creating reference SIMs that contain comprehensive test data can be time consuming and

difficult to accomplish. This paper describes an approach for automating the population of test data onto SIMs to create reference material for use in tool validation. It also covers details of the implementation and explains characteristics of SIMs that pertain to the solution.

The Global System for Mobile Communications (GSM) standards for cellular networks were originally developed by the European Conference of Postal and Telecommunications Administrations, continued by the European Telecommunications Standards Institute and then by the 3rd Generation Partnership Project (3GPP), where they are now maintained. Commercial GSM service was started in mid-1991. By 1993, thirty-six GSM networks were operating in twenty-two countries. Although begun in Europe, GSM has become a broader international standard with compliant networks operational in more than 200 countries around the world, including North America.

Subscriber Identity Modules (SIMs) are synonymous with mobile phones and devices that interoperate with GSM cellular networks. Under the GSM framework, a cellular phone is referred to as a Mobile Station and is partitioned into two distinct components: the Subscriber Identity Module (SIM) and the Mobile Equipment (ME). As the name implies, a SIM is a removable component that contains essential information about the subscriber. The ME, the remaining radio handset portion, cannot function fully without one. The SIM's main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. The SIM also provides a store for personal information, such as phone book entries and text messages, as well as operational information, such as that involving location.

SIMs are often classified according to the phase of the specifications supported, which is recorded in an element of its file system. The three phases defined are phase 1, phase 2 and phase 2+, which correspond roughly to first, second and 2.5 generation network facilities. Another class of SIMs being deployed in third generation (3G) Universal Mobile Telecommunications Service (UMTS) networks is UMTS SIMs (USIMs). USIMs are enhanced versions of present-day SIMs, containing backward-compatible information.

Some of the earliest, general purpose, forensic tools for mobile phones targeted SIMs, not only because of detailed specifications available for them, but also because of the highly relevant and useful digital evidence that could be recovered. A recent assessment of the capabilities of present day forensic tools to recover evidence from SIMs, however, noted discrepancies between the test data placed on a SIM and that recovered and reported in every tool. They include the inability to recover any data from certain SIMs, inconsistencies between the data displayed on screen to the user and that generated in the output reports, missing truncated data in reported or displayed output, errors in the decoding and translation of recovered data and the inability to recover all relevant data. Furthermore, updates or new versions of a tool, on occasion, performed less capably than a previous version.

Validating a forensic SIM tool is an essential quality assurance measure. The results aid in deciding how to compensate for any noted shortcomings or whether to switch to a new version of the tool. Validation should be carried out when first choosing a forensic tool to ensure its acceptability and redone when updates or new versions of the tool become available to maintain consistency of results. Validating a tool entails defining a comprehensive test data set, loading it onto the device and following procedures to acquire and recover the test data. While tool validation is essential, building reference SIMs that contain comprehensive test data can be time consuming and difficult to carry out, requiring the use of various SIM editing tools and handsets to populate the data. In addition, variances exist between SIMs

from different manufacturers, such as different file capacities allocated for entries (e.g. the phonebook) and different size data fields supported (e.g. an individual's name in a phonebook entry). Different character encodings may also apply to the various languages of interest. This paper discusses an approach for automating the population of reference test data onto SIMs that attempts to address those types of differences. Details of the implementation are also covered.

2.4.1 Sim Characteristics

The SIM-ME partitioning of a cell phone stipulated in the GSM standards has brought about a form of portability. Moving a SIM between compatible cell phones automatically transfers with it the subscriber's identity and the associated information and capabilities. In contrast, many of the present-day phones that follow Code Division Multiple Access (CDMA) standards (i.e. TIA/EIA/IS-95-A and B) initially did not employ a SIM. Instead, analogous SIM functionality was incorporated directly within the device. While SIMs are most widely used in GSM systems, comparable modules are also used in Integrated Digital Enhanced Network (iDEN) phones, which use a proprietary mobile communications technology developed by Motorola and phones used in UMTS networks (i.e. a USIM). Because of the flexibility a SIM offers GSM phone users to port their identity, personal information and service between devices, eventually all cellular phones are expected to include (U)SIM-like capability. For example, requirements for a Removable User Identity Module (R-UIM), as an extension of SIM capabilities, have been specified for cellular environments conforming to TIA/EIA/IS-95-A and B specifications, which include Wideband Spread Spectrum based CDMA.

At its core, a SIM is a special type of smart card that typically contains a processor and between 16 and 256 KB of persistent electronically erasable, programmable read only memory (EEPROM). It also includes random access memory (RAM) for program execution and read only memory (ROM) for the operating system, user authentication and data encryption algorithms and other applications. The hierarchically organized file system of a SIM resides in persistent memory and stores such things as names and phone number entries, text messages and network service settings. Depending on the phone used, some information on the SIM may coexist in the memory of the phone. Alternatively, information may reside entirely in the memory of the phone instead of available memory on the SIM.

Authenticating a device to a network securely is a vital function performed via the SIM. Cryptographic key information and algorithms within the tamper resistant-module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information that could be used to clone the SIM and gain access to a subscriber's services. Cryptographic key information in the SIM also supports stream cipher encryption to protect against eavesdropping on the air interface.

Two sizes of SIMs have been standardized, but only the smaller size shown in Fig. 2 is broadly used in GSM phones today. The module has a width of 25 mm, a height of 15 mm and a thickness of .76 mm, which is roughly the footprint of a postage stamp. Although similar in dimension to a MiniSD or MMCmobile removable memory card supported by some cell phones, SIMs follow a different set of specifications with vastly different characteristics. For example, their 8-pin connectors are not aligned along a bottom edge as with removable media cards, but instead form a circular contact pad integral to the smart card chip, which is embedded in a plastic frame. Also, the slot for the SIM card is normally not accessible from the exterior of the phone to facilitate frequent insertion and removal as with a memory card and instead, is typically found in the battery compartment under the battery.

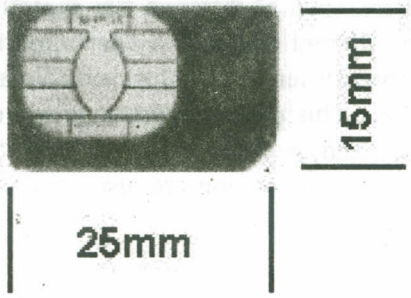


Fig. 2: Subscriber Identity Module

When a SIM is inserted into a phone handset and pin contact is made, a serial interface is used for communicating between them. A SIM can be removed from a phone and read using a specialized SIM card reader and software through the same interface. Standard-size smart card adapters are also available for SIMs, which allows them to be inserted into and read with a conventional smart card reader.

The SIM File System

Forensic SIM tools extract digital evidence present in the file system of a SIM. The file system is organized in a hierarchical tree structure, as shown in Fig. 3. It is composed of the following three types of elements:

- Master File (MF) – the root of the file system that contains dedicated and elementary files.
- Dedicated File (DF) – a subordinate directory to the master file that contains dedicated and elementary files.
- Elementary File (EF structured as either a or a fixed set of fixe

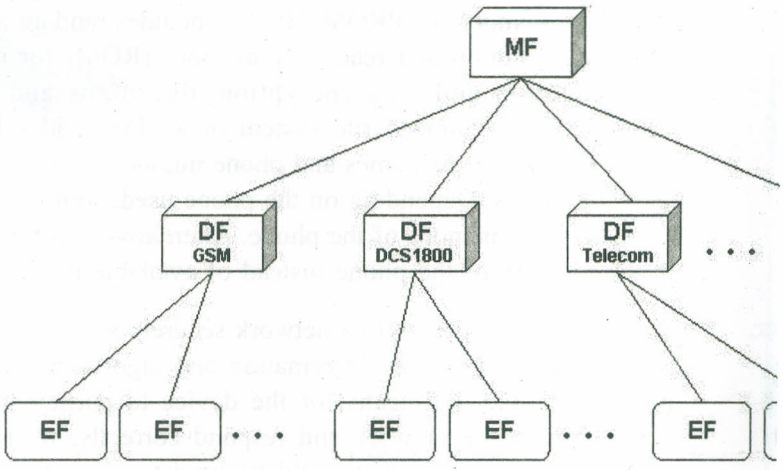


Fig. 3: SIM File System

The GSM standards define several important dedicated files immediately under the MF: DFGSM, DFDCS1800 and DFTELECOM. Several EFs are defined for these DFs and the MF, including many that are mandatory. The EFs under DFGSM and DFDCS1800 contain mainly network-related information respectively for GSM 900 MHz and Digital Cellular System (DCS) 1800 MHz band operation. EFs for 850 MHz and 1900 MHz bands used in North America are found respectively under those DFs as well and typically contain identical information. The EFs under DFTELECOM contain service-related information.

Though SIM file systems are highly standardized, the standards allow flexibility such that their content can vary among network operators and service providers. For example, a network operator might not use an optional file system element, might create an additional element on the SIM for use in its operations or might install a built-in function to provide a specialized service.

File Access Controls

SIMs, as with smart cards in general, employ a range of tamper resistance techniques to protect their contents. In addition, various levels of rights exist that are assigned to a DF or EF to control the conditions of access:

- Always – Access can be performed without any restriction.
- Card Holder Verification 1 (CHV1) – Access can be performed only after a successful verification of the user's PIN or if PIN verification is disabled.
- Card Holder Verification 2 (CHV2) – Access can be performed only after a successful verification of the user's PIN2 or if PIN2 verification is disabled.
- Administrative – Access can be performed only after prescribed requirements for administrative access are fulfilled.
- Never – Access of the file over the SIM/ME interface is forbidden.

The SIM operating system controls access to an element of the file system based on its access condition and the type of action being attempted. For example, actions on EFs include searching, reading and updating the contents. While reading and searching the contents of a particular EF might be allowed without CHV1 verification (i.e. an Always access condition), updating might likely require as a prerequisite CHV1 being correctly verified (i.e. a CHV1 access condition). In general, CHV1 protects core SIM data for the card user against unauthorized reading and updating, while CHV2 protects administrative dialling control data mainly for a card manager (e.g. the parent of a child user), if such a relationship exists. The 4 to 8 digit values of both CHVs can be reset by anyone knowing the PIN values or their verification completely disabled. So-called ADM Codes are required for Administrative access and are normally kept by the service provider or network operator that issued the SIM.

The SIM operating system allows only a preset number of attempts, usually three, to enter the correct CHV before further attempts are blocked. Submitting the correct Unblock CHV value, also known as a PIN Unblocking Key (PUK), resets the CHV and the attempt counter. If the identifier of the SIM (i.e. its Integrated Circuit Chip Identifier or ICCID) is known, the Unblock CHV for either CHV1 or CHV2 can be obtained from the service provider or network operator. The ICCID is normally imprinted on the SIM along with the name of the network provider. If needed, the identifier can also be read with a SIM tool from an EF, EFICCID, since the Always access condition applies by definition. If the number of attempts to enter an Unblock CHV value correctly exceeds a set limit, normally ten attempts, the card becomes blocked permanently.

2.5 DIGITAL EVIDENCE

An assortment of digital evidence from a SIM lies scattered throughout various EFs in the file system. News articles of high profile cases occasionally contain illustrative examples where evidence recovered from a SIM was used successfully in an investigation.

- Text Message and Call Data
- Location Data

For a reference SIM to be useful in validating forensic SIM tools, its file system must be populated with test data that is normally recovered by such tools. Several general categories of evidence can be identified:

- Service-related Information
- Phonebook and Call Information
- Messaging Information
- Location Information.

A number of EFs from each of these categories whose information is regularly employed by forensic specialists are discussed below as examples of core elements for validation.

2.5.1 Service-Related Information

The Integrated Circuit Card Identification (ICCID) is a unique numeric identifier for the SIM that can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number and an individual account identification number.

Aside from the prefix, the components of an ICCID are variable, making them sometimes difficult to interpret. The ICCID can "Always" be read from the SIM without providing a PIN and can never be updated. The country code and issuer identifier can be used to determine the network operator providing service and obtain call data records for the subscriber.

The International Mobile Subscriber Identity (IMSI) is a unique 15-digit numeric identifier assigned to the subscriber. It has a somewhat similar structure to the ICCID: a Mobile Country Code (MCC), a Mobile Network Code (MNC) and a Mobile Subscriber Identity Number (MSIN) assigned by the network operator. The MCC is 3 digits, while the MNC may be either 2 or 3 digits, with the MSIN taking up the remainder. The fourth byte of another EF, Administrative Data (AD), gives the length of the MNC. Networks use IMSIs to determine which network a device owner subscribes to and, if not their network, whether to allow those network subscribers to access service.

The ICCID and IMSI can be used reliably to identify the subscriber and the network operator providing service. Since these identifiers can be misinterpreted, however, other SIM data can help confirm a finding.

The Mobile Station International Subscriber Directory Number (MSISDN) is intended to convey the telephone number assigned to the subscriber for receiving calls on the phone. Unlike the ICCID and IMSI, however, the MSISDN is an optional EF. If present, its value can be updated by the subscriber, making it a less reliable data source, since it would then be inconsistent with the actual number assigned.

The Service Provider Name (SPN) is an optional EF that contains the name of the service provider. If present, it can be updated only by the administrator (i.e. Administrator access). Similarly, the Service Dialling Numbers (SDN) EF contains numbers of special services such as customer care and, if present, can help identify to which network the SIM is registered. The Extension3 (EXT3) EF contains additional data for an SDN entry.

2.5.2 Phonebook and Call Information

The Abbreviated Dialling Numbers (ADN) EF retains a list of names and phone numbers entered by the subscriber. The type of number (TON) and numbering

plan identification (NPI) are also maintained in this EF. The storage permits rudimentary phonebook operation by providing the means to select commonly dialled phone numbers by name and update or call them using a menu or certain keys on the phone. If the ADN storage capacity is insufficient to hold all of the information for an entry (e.g. an unusually long sequence of digits), an index to an Extension1 (EXT1) EF record is used to link to where the additional data is maintained. Most SIMs provide around 100 slots for ADN entries.

The Fixed Dialling Numbers (FDN) EF is similar to ADN insofar as a list of names and phone numbers is involved. However, this list is used only in situations where the user is restricted to dialling just the numbers prescribed by a card manager. If the FDN storage capacity cannot hold all of the information for an entry, an index to an Extension2 (EXT2) EF record is used to indicate where the additional data is maintained.

The Last Numbers Dialled (LND) EF contains a list of the most recent phone numbers called by the device. A name may also be associated with an entry (e.g. a called phonebook entry) and stored with the number. Though a number appears on the list, a connection may not have been successful, only attempted. Most SIMs provides only a limited number of slots (e.g. ten) for these entries. If the LND storage capacity cannot hold all of the information for an entry, an index to an EXT1 EF record indicates where the additional data is maintained. Some phones do not store called numbers on the SIM and instead rely on their own memory for storage.

2.5.3 Messaging Information

Text messaging is a means of communication in which messages entered on one cell phone are sent to another via the mobile phone network. The Short Message Service (SMS) EF contains text and associated parameters for messages received from or sent to the network or are to be sent out as an MS-originated message. SMS entries contain other information besides the text itself, such as the time an incoming message was sent, as recorded by the mobile phone network, the sender's phone number, the SMS Centre address and the status of the entry. The status of a message entry can be designated as unoccupied free space or as occupied by one of the following: a received message to be read, a received message that has been read, an outgoing message to be sent or an outgoing message that has been sent. Messages deleted via the phone interface are often simply designated as free space and the content retained unchanged on the SIM until they are overwritten. When a new message is written to an available slot, the unused portion is filled with padding, overwriting any remnants of a previous message that might be there.

The capacity for stored messages varies among SIMs. Many cell phones also use their own internal memory for storing text messages. The choice of memory where messages are stored (i.e. SIM or phone) can vary depending on the phone software and user settings. For example, a default arrangement might be for all incoming messages to be stored on the memory of the SIM before using internal phone memory, while outgoing messages are stored only if explicitly requested. Phone models of a particular generation and manufacturer often behave consistently in this respect.

The maximum length of a single SMS message entry is 160 characters of text. Messages exceeding that length must be broken down into smaller segments by the sending phone and reassembled by the receiving phone. This feature is especially useful for foreign language character sets such as Chinese or Arabic whose encoding consumes considerably more bits per character than English. A reference number parameter identifies the entries whose segments require reassembly. Such messages are referred to as concatenated messages. SMS messages may originate through other means than a cell phone, such as from an Internet SMS server or through electronic mail.

An SMS message can be coded in different ways. The original and most common encoding scheme is a GSM-specific 7-bit character set packed into a bit stream. Such an encoding cannot be interpreted readily by individuals using a hex editor, nor can it embody all languages. Support for other character sets, such as 16-bit Unicode, was added for languages whose alphabets cannot be represented using the original Western European character set.

An Enhanced Messaging Service (EMS) was defined as a way to extend SMS message content to allow simple multimedia messages to be conveyed. EMS messages can contain not only formatted text with different font styles and fonts, but also black and white bitmap pictures and monophonic melodies. EMS message content resides in the SMS EF along with SMS message content. EMS messaging is essentially an application-level content extension to SMS, which conforms to the general SMS message structure and support for concatenated messages.

EMS-enabled devices are backward compatible by definition with SMS-enabled devices.

2.5.4 Location Information

A GSM network consists of distinct radio cells used to establish communications with mobile phones. Cells are grouped together into defined areas used to manage communications. Phones keep track of the area under which they fall for both voice and data communications. The Location Information (LOCI) EF contains the Location Area Information (LAI) for voice communications. The LAI is composed of the MCC and MNC of the location area and the Location Area Code (LAC), an identifier for a collection of cells. When the phone is turned off, the LAI is retained, making it possible to determine the general locale where the phone was last operating. Because a location area can contain hundreds or more cells, the locale can be quite broad. However, it can nevertheless be useful in narrowing down the region where the event occurred.

Similarly, the GPRS Location Information (LOCIGPRS) EF contains the Routing Area Information (RAI) for data communications over the General Packet Radio Service (GPRS). The RAI is composed of the MCC and MNC of the routing area and the LAC, as well as a Routing Area Code (RAC), an identifier of the routing area within the LAC. Routing areas may be defined the same as location areas or they may involve fewer cells, providing greater resolution.

Forensic examination of cell phones is a growing subject area in computer forensics. Identity modules play an important role in this process. Forensic examination tools for phone handsets and identity modules translate data to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence. However, tools may contain some degree of inaccuracy. For example, the tool's implementation may contain a programming error; a specification used by the tool to translate encoded bits into data comprehensible by the examiner may be inexact or out of date; or the protocol used to access the SIM may be incorrect, causing the tool to function improperly in certain situations.

The failure of a forensic tool to correctly recover and report relevant SIM data greatly impedes the ability of the forensics specialist and jeopardizes the credibility of the overall results. While experience with a forensic tool provides an understanding of its limitations, it does not replace the need to validate the tool's capabilities, particularly for the initial and subsequent versions of a tool selected for use and when patches or updates are applied to the tool or the tool's operating environment. Quality measures should always be applied to ensure that results remain consistent and any variations understood. This principle applies both to forensic specialists that use such tools and forensic tool manufacturers who produce them.

Suitable reference materials are essential for validating a forensic tool. However, creating suitable reference materials can be problematic and time consuming. The technique outlined in this paper provides a means to create reference material automatically for SIM tool validation, based on selected sets of test data. The technique was implemented in the Java programming language and the test data represented in XML to provide a high degree of platform independence. The resulting program is relatively straightforward to use and requires only a minimal amount of additional equipment (i.e. a PC/SC compatible card reader) to populate a SIM for use in tool validation.

Fig. 4 gives an overview of the hardware characteristics of basic, advanced and high-end cell phones for display quality, processing and storage capacity, memory and I/O expansion, built-in communications and video and image capture. The bottom of the diagram shows the range of cellular voice and data advances from kilobit analog networks, still in use today, to megabit 3rd generation digital networks in the planning and early deployment stages. The diagram attempts to illustrate that more capable phones can capture and retain not only more information, but also more varied information, through a wider variety of sources, including removable memory modules, other wireless interfaces and built-in hardware. Note that hardware components can and do vary from those assignments made in the diagram and, over time, technology once considered high end or advanced eventually appears in what would then be considered a basic phone. Nevertheless, the principle remains true.

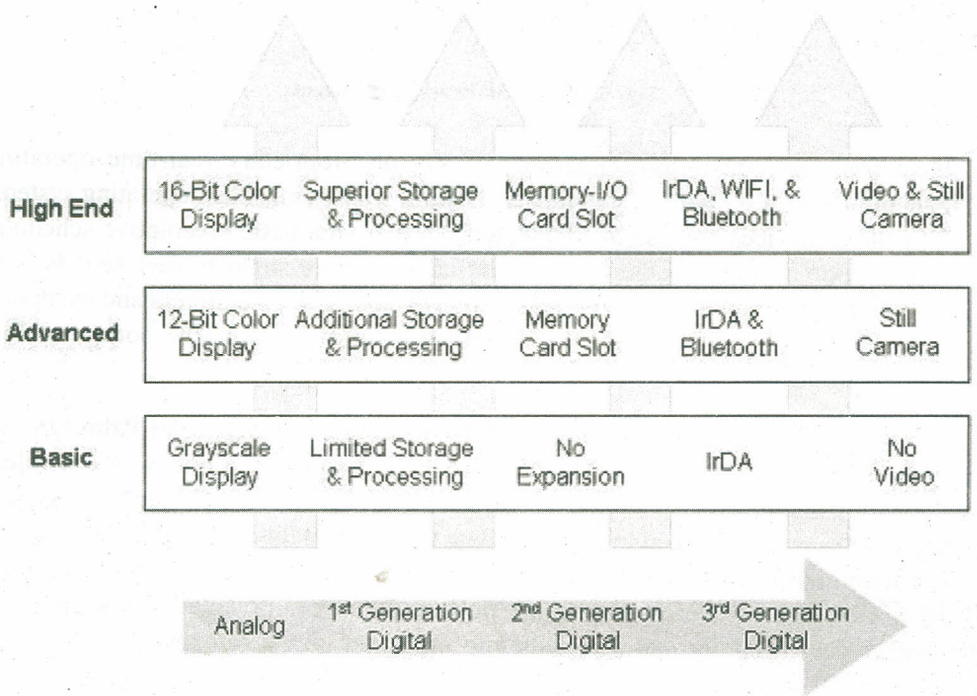


Fig. 4: Phone Hardware Components

Just as with hardware components, software components involved in communications vary with the class of phone. Basic phones normally include text messaging using the Short Message Service (SMS). An advanced phone might add the ability to send simple picture messages or lengthy text messages using the Extended Message Service (EMS), while a high-end phone typically supports the Multimedia Message Service (MMS) to exchange sounds, color images and text. Similarly, the ability to chat on-line directly with another user may be unsupported, supported through a dedicated SMS channel or supported with a full Instant Messaging (IM) client. High-end phones typically support full function email and Web clients that respectively use POP (Post Office Protocol)/IMAP (Internet Message Access Protocol)/SMTP (Simple Mail Transfer Protocol) and HTTP, while advanced phones provide those services via WAP (Wireless Application Protocol)

and basic phones do not include any support. Fig. 5 gives an overview of the capabilities usually associated with each class of phone.

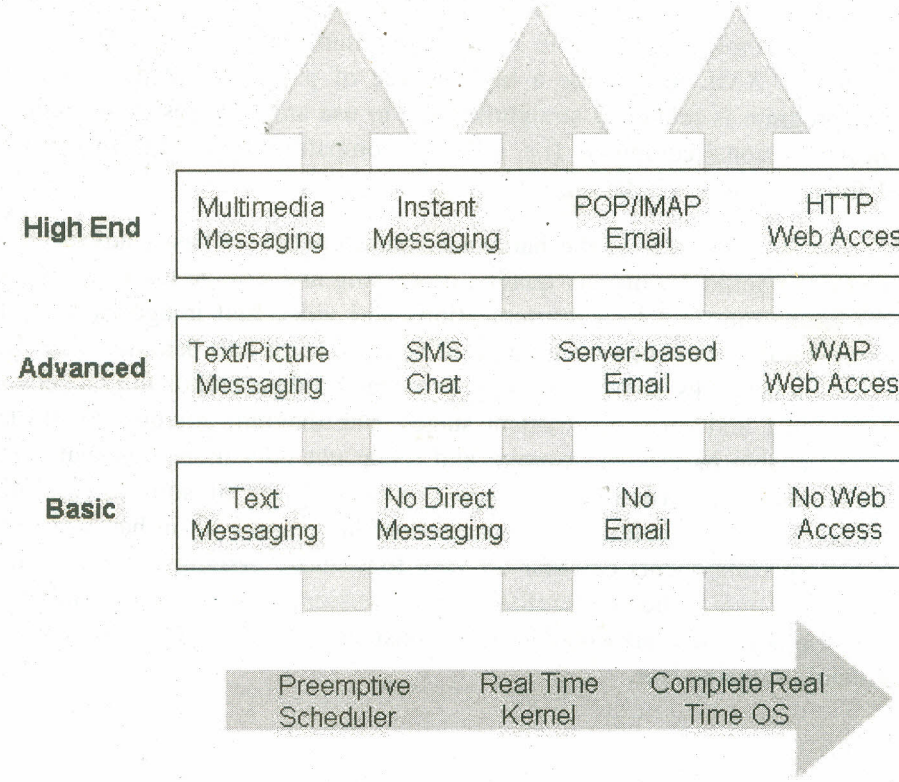


Fig. 5: Phone Software Components

Most basic and many advanced phones rely on proprietary real-time operating systems developed by the manufacturer. Commercially embedded operating systems for cellular devices are also available that range from a basic preemptive scheduler with support for a few other key system calls to more sophisticated kernels with scheduling alternatives, memory management support, device drivers and exception handling, to complete embedded real-time operating systems. The bottom of Fig. 5 illustrates this range.

Many high-end smart phones have a PDA heritage, evolving from Palm OS and Pocket PC (also known as Windows mobile) handheld devices. As wireless telephony modules were incorporated into such devices, the operating system capabilities were enhanced to accommodate the functionality. Similarly, the Symbian OS found on many smart phones also stems from an electronic organizer heritage. RIM OS devices, which emphasize push technology for email messaging, are another device family that also falls into the smart phone category.

2.6 SUBSCRIBER IDENTITY MODULE

Another useful way to classify cellular devices is by whether they involve a Subscriber Identity Module (SIM). A SIM is removable card designed for insertion into a device, such as a handset. SIMs originated with a set of specifications originally developed by the CEPT (Conference of European Posts and Telecommunications) and continued by ETSI (the European Telecommunications Standards Institute) for GSM networks. GSM standards mandate the use of a SIM for the operation of the phone. Without it, a GSM phone cannot operate. In contrast, present-day CDMA phones do not require a SIM. Instead, SIM functionality is incorporated directly within the device.

A SIM is an essential component of a GSM cell phone that contains information particular to the user. A SIM is a special type of smart card that typically contains

between 16 to 64 KB of memory, a processor and an operating system. A SIM uniquely identifies the subscriber, determines the phone's number and contains the algorithms needed to authenticate a subscriber to a network. A user can remove the SIM from one phone, insert it into another compatible phone and resume use without the need to involve the network operator. The hierarchically organized filesystem of a SIM is used to store names and phone numbers, received and sent text messages and network configuration information. Depending on the phone, some of this information may also coexist in the memory of the phone or reside entirely in the memory of the phone instead of the SIM. While SIMs are most widely used in GSM systems, compatible modules are also used in IDEN phones and UMTS user equipment (i.e. a USIM). Because of the flexibility SIM offers GSM phone users to port their identity and information between devices, eventually all cellular phones are expected to include SIM capability.

Though two sizes of SIMs have been standardized, only the smaller size shown at left is broadly used in GSM phones today. The module has a width of 25 mm, a height of 15 mm and a thickness of .76 mm, which is roughly the size of a postage stamp. Its 8-pin connectors are not aligned along a bottom edge as might be expected, but instead form a circular contact pad integral to the smart card chip, which is embedded in a plastic frame. Also, the slot for the SIM card is normally not accessible from the exterior of the phone as with a memory card. When a SIM is inserted into a phone and pin contact is made, a serial interface is used to communicate with the computing platform using a half-duplex protocol. SIMs can be removed from a phone and read using a specialized SIM card reader and software. A SIM can also be placed in a standard-size smart card adapter and read using a conventional smart card reader.

As with any smart card, its contents are protected and a PIN can be set to restrict access. Two PINs exist, sometimes called PIN1 and PIN2 or CHV1 and CHV2. These PINs can be modified or disabled by the user. The SIM allows only a preset number of attempts, usually three, to enter the correct PIN before further attempts are blocked. Entering the correct PUK (PIN Unblocking Key) resets the PIN number and the attempt counter. The PUK can be obtained from the service provider or the network operator based on the SIM's identity (i.e. its ICCID). If the number of attempts to enter the PUK correctly exceeds a set limit, normally ten attempts, the card becomes blocked permanently.

2.7 REMOVAL MEDIA

Removable media extends the storage capacity of a cell phone, allowing individuals to store additional information beyond the device's built-in capacity. They also provide another avenue for sharing information between users that have compatible hardware. Removable media is non-volatile storage, able to retain recorded data when removed from a device. The main type of removable media for cell phones is a memory card. Though similar to a SIM in size, they follow a different set of specifications and have vastly different characteristics. Some card specifications also allow for I/O capabilities to support wireless communications (e.g. Bluetooth or WiFi) or other hardware (e.g. a camera) to be packaged in the same format.

A wide array of memory cards exists on the market today for cell phones and other mobile devices. The storage capacities of memory cards range from megabytes (MB) to gigabytes (GB) and come in sizes literally as small as a thumbnail. As technological advances continue, such media is expected to become smaller and offer greater storage densities. Fortunately, such media is normally formatted with a conventional filesystem (e.g. FAT) and can be treated similarly to a disk drive, imaged and analyzed using a conventional forensic tool with a compatible media adapter that supports an Integrated Development Environment (IDE) interface. Such

adapters can be used with a write blocker to ensure that the contents remain unaltered. Below is a brief overview of several commonly available types of memory cards used with cell phones.

- **Multi-Media Cards (MMC)**

A Multi-Media Card (MMC) is a solid-state disk card with a 7-pin connector. MMC cards have a 1-bit data bus. They are designed with flash technology, a non-volatile storage technology that retains information once power is removed from the card. Multi-Media Cards are about the size of a postage stamp (length-32 mm, width-24 mm and thickness-1.4 mm). Reduced Size Multi-Media cards (RS-MMC) also exist. They are approximately one-half the size of the standard MMC card (length-18mm, width-24mm and thickness-1.4mm). An RS-MMC can be used in a full-size MMC slot with a mechanical adapter. A regular MMC card can be also used in an RS-MMC card slot, though part of it will stick out from the slot. MMCplus and MMCmobile are higher performance variants of MMC and RS-MMC cards respectively that have a 13-pin connector and an 8-bit data bus.

- **Secure Digital (SD) Cards**

Secure Digital (SD) memory cards (length-32 mm, width-24 mm and thickness-2.1mm) are comparable to the size and solid-state design of MMC cards. In fact, SD card slots can often accommodate MMC cards as well. However, SD cards have a 9-pin connector and a 4-bit data bus, which afford a higher transfer rate. SD memory cards feature an erasure-prevention switch. Keeping the switch in the locked position protects data from accidental deletion. They also offer security controls for content protection (i.e. Content Protection Rights Management). MiniSD cards are an electrically compatible extension of the existing SD card standard in a more compact format (length-21.5 mm, width-20 mm and thickness-1.4 mm). They run on the same hardware bus and use the same interface as an SD card and also include content protection security features, but have a smaller maximum capacity potential due to size limitations. For backward compatibility, an adapter allows a MiniSD Card to work with existing SD card slots.

- **Memory Sticks**

Memory sticks provide solid-state memory in a size similar to, but smaller than, a stick of gum (length-50mm, width-21.45mm, thickness-2.8mm). They have a 10-pin connector and a 1-bit data bus. As with SD cards, memory sticks also have a built-in erasure-prevention switch to protect the contents of the card. Memory Stick PRO cards offer higher capacity and transfer rates than standard Memory Sticks, using a 10-pin connector, but with a 4-bit data bus. Memory Stick Duo and Memory Stick PRO Duo, smaller versions of the Memory Stick and Memory Stick PRO, are about two-thirds the size of the standard memory stick (length-31mm, width-20mm, thickness-1.6mm). An adapter is required for a Memory Stick Duo or a Memory Stick PRO Duo to work with standard Memory Stick slots.

- **TransFlash**

TransFlash is a tiny memory card based on the MiniSD card. Because of their extremely small size (length-15 mm, width-11 mm and thickness-1 mm), frequent removal and handling is discouraged, making them more of a semi- removable memory module. TransFlash cards have an 8-pin connector and a 4-bit data bus. An adapter allows a TransFlash card to be used in SD-enabled devices. Similarly, the newly announced MMCmicro device is another ultra small card (length-14 mm, width-12 mm and thickness-1.1 mm), compatible with MMC-enabled devices via an adapter. MMCmicro cards have a 10-pin connector and a 1 or 4-bit data bus. TransFlash has recently been renamed MicroSD.

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Write a note on multi-media cards.

.....

.....

.....

.....

.....

2.8 LET US SUM UP

This unit deals with the "Analysis of CDR's".Call Detail Record (CDR) can contain information that the mobile network operator uses for subscriber identification, call charging, services obtained, call routing etc. It also covers types of Call Data and explained SIM Card Analysis and SIM Characteristics.

2.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

Multi-Media Card

A Multi-Media Card (MMC) is a solid-state disk card with a 7-pin connector. MMC cards have a 1-bit data bus. They are designed with flash technology, a non-volatile storage technology that retains information once power is removed from the card. Multi-Media Cards are about the size of a postage stamp (length-32 mm, width-24 mm and thickness-1.4 mm). Reduced Size Multi-Media cards (RS-MMC) also exist. They are approximately one-half the size of the standard MMC card (length-18mm, width-24mm and thickness-1.4mm). An RS-MMC can be used in a full-size MMC slot with a mechanical adapter. A regular MMC card can be also used in an RS-MMC card slot, though part of it will stick out from the slot. MMCplus and MMCmobile are higher performance variants of MMC and RS-MMC cards respectively that have a 13-pin connector and an 8-bit data bus.

UNIT 3 APPLICATION OF SIM CARD READER'S

Structure

3.0 INTRODUCTION

This unit covers various applications of SIM Card reader's. The Synopsis of SIMIS, Synopsis of ForensicSIM, Synopsis of Forensic Card Reader, Synopsis of SIMCon are discussed in detail.

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- understand various applications of SIM Card readers; and
- explain criteria for choosing the tool.

3.2 APPLICATION OF SIM CARD READER'S

3.2.1 SIM Card Acquisition

TULP2G version 1.2.0.2 gives examiners the ability to acquire SIM card data using a PC/SC-compatible reader. The acquisition steps followed to acquire data directly from the SIM are the same as acquiring data from a phone, except for selecting PC/SC Chip Card Communication versus a serial or socket. The data fields acquired (e.g. Abbreviated Dialing Numbers, Last Numbers Dialed, Fixed Dialing Numbers, Messages etc.) are dependent upon the SIM and service provider. The Report facilities operate in a similar fashion as for phone acquisitions, described above.

Table below summarizes the results from applying the scenarios listed at the left of the table to the SIMs across the top.

Scenario	SIM		
	5343	8778	1144
Basic Data	Meet	Meet	Meet
Location Data	Below	Below	Below
EMS Data	Meet	Meet	Below
Foreign Language Data	Meet	Meet	Meet

3.2.2 Synopsis of SIMIS

SIMIS version 2.0.13 from Crown Hill is able to acquire information from SIM cards via the PC/SC-compatible card reader that comes with the software. SIMIS provides examiners with a user interface containing a set of tabs providing examiners with the ability to create report notes, import archived reports, search acquired data and PIN administration. SIMIS allows the following data types to be acquired from SIM cards: Abbreviated Dial Numbers (ADN), Fixed Dial Numbers (FDN), International Mobile Subscriber Identity (IMSI), Last Numbers Dialed (LND), Mobile Subscriber Integrated Services Digital Network Number (MSISDN), Short Message Server Parameters (SMSP), SMS Short Messages, Deleted Messages, Public Land Mobile Networks (PLMNS), Forbidden Public Land Mobile Networks (FPLMNS), Location Information, Broadcast Control Channel (BCCH), Cell Broadcast Message Identifier for Data Download (CBMID), Voicemail Number, Integrated Circuit Card Identification (ICCID), Phase ID, Service Provider, Administration Data, Service Dialing Number (SDN) and Capability Configuration Parameters. The tool can also perform a full dump of the card contents for analysis.

Acquisition Stage

The acquisition stage begins by prompting the examiner to select the interface to be used as illustrated below.

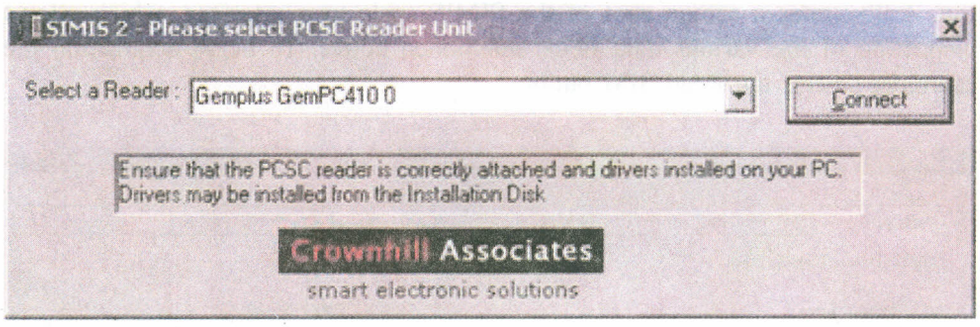


Fig. 1

After the correct PIN number has been entered, the examiner can Change, Unlock, Activate or Deactivate the PIN from the user interface, as illustrated in Fig. 2 below.

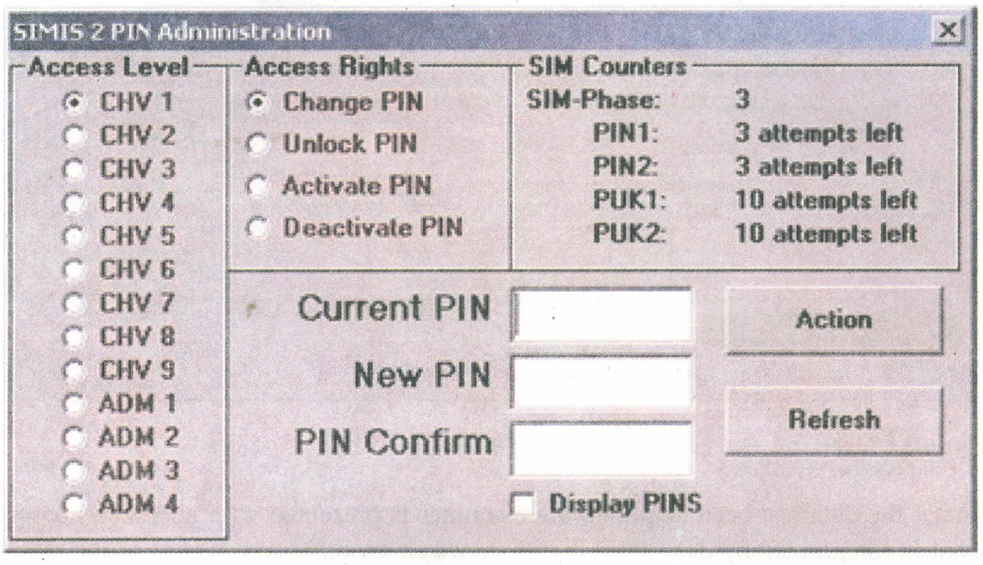


Fig. 2

The acquisition begins by collecting some information related to the case (i.e. unique file reference, operator name, case number, IMEI, ICCID and Service Provider information found on the SIM) from the examiner that is included in the final report. After a successful acquisition, SIMIS compares the data manually entered (e.g. the ICCID) with the data collected from the SIM for consistency. If a discrepancy is found, the examiner is informed of the inconsistency as illustrated below in Fig. 3.

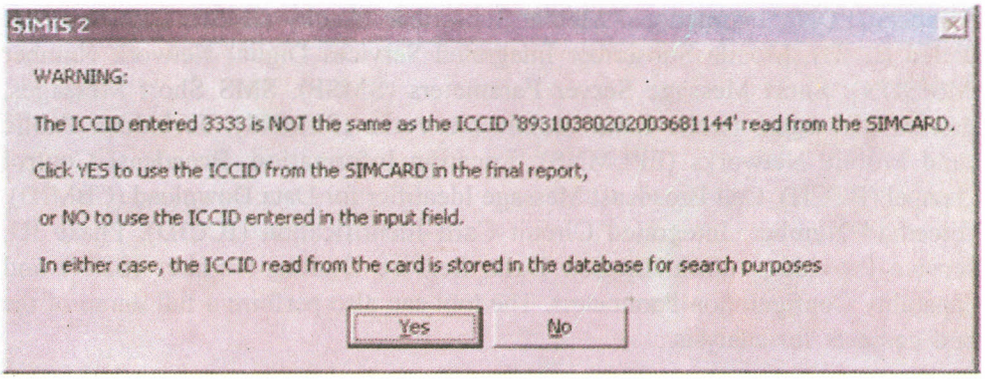


Fig. 3

Fig. 4 illustrates a screen shot of the SIMIS table user interface, which allows inspection of the various data fields mentioned above. To begin acquisition the examiner selects the Read SIM button.

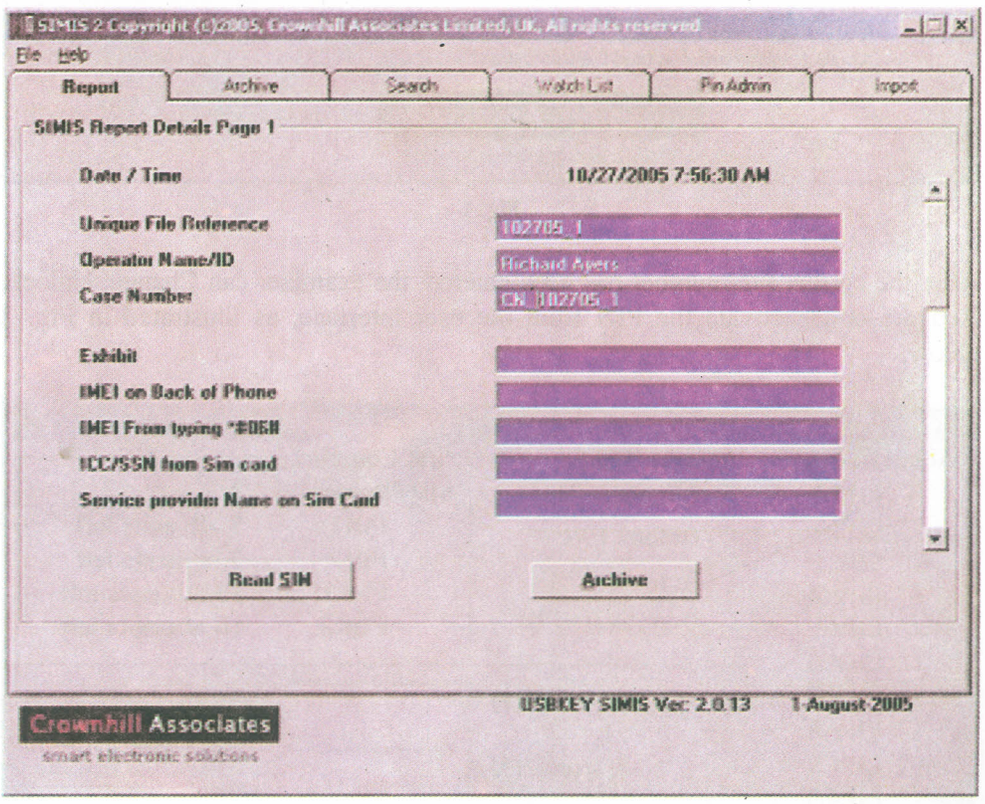


Fig. 4

After the data has been acquired, the examiner is presented with an HTML report that is categorized by data item. Fig. 5 shows an example screen shot of the menu guided HTML generated report and the ADN entries.

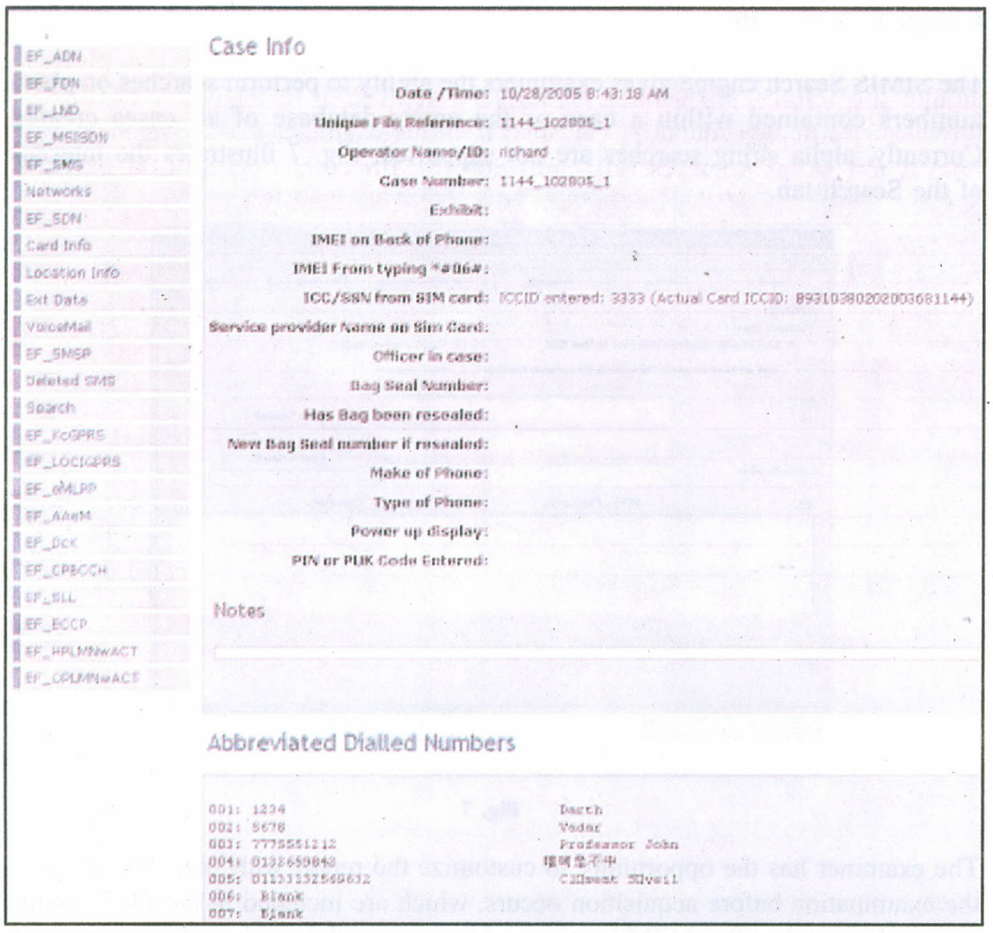


Fig. 5

After a successful acquisition, SIMIS allows MD5 hashes to be generated ensuring the integrity of the data. MD5 and SHA2 hashes can be created for the SIMIS2 executable, proprietary SIMIS case file, report files and log files, as illustrated below in Fig. 6.

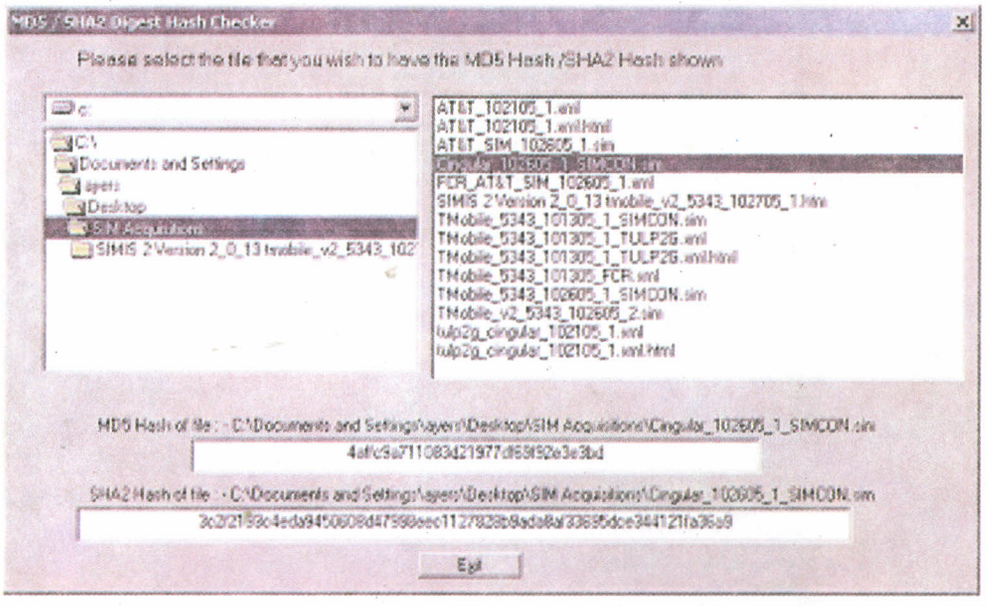


Fig. 6

SIMIS allows examiners to view additional data that is not displayed within the GUI interface. An ASCII dump file (.dmp) can be created in the directory where the SIMIS output data resides by selecting "SIM dump" from the File menu. For example, Forbidden Networks (FPLMNs) can be obtained this way.

Search Functionality

The SIMIS Search engine gives examiners the ability to perform searches on phone numbers contained within a case or the entire database of all cases created. Currently, alpha string searches are not supported. Fig. 7 illustrates the interface of the Search tab.

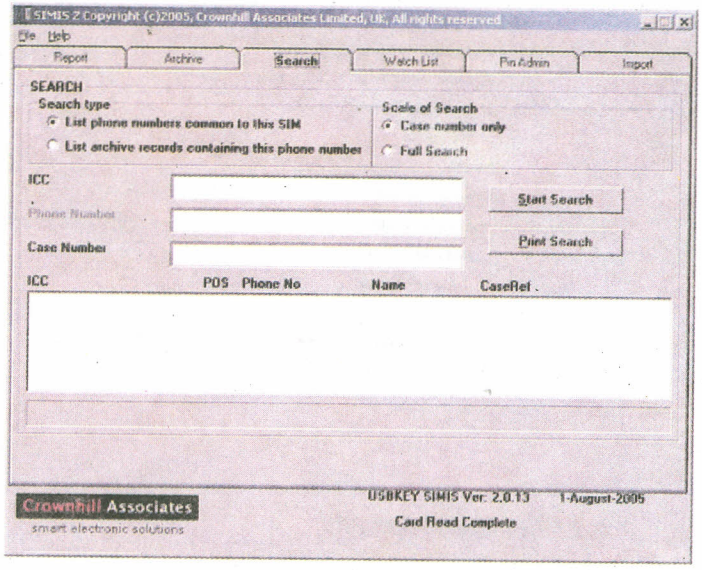
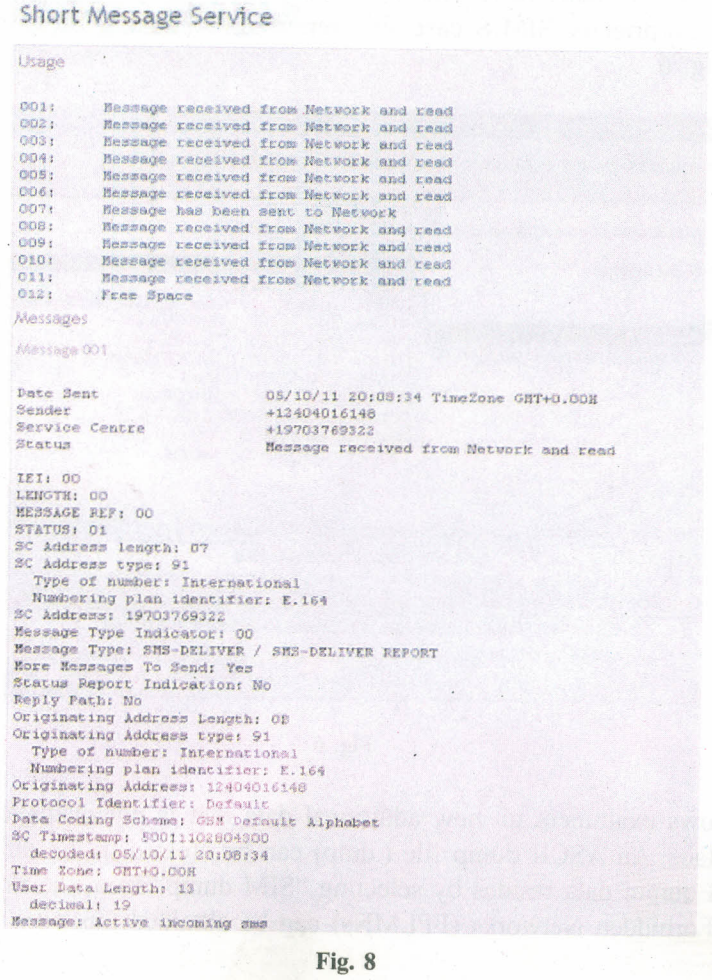


Fig. 7

The examiner has the opportunity to customize the report with specifics related to the examination before acquisition occurs, which are included in the final version. After selecting the "Read SIM" option and acquiring all data, the report is generated is displayed to the user. The generated report is an HTML-based report that can be viewed with a standard HTML editor. Fig. 8 shows an excerpt of the generated report.



Short Message Service

Usage

```
001:    Message received from Network and read
002:    Message received from Network and read
003:    Message received from Network and read
004:    Message received from Network and read
005:    Message received from Network and read
006:    Message received from Network and read
007:    Message has been sent to Network
008:    Message received from Network and read
009:    Message received from Network and read
010:    Message received from Network and read
011:    Message received from Network and read
012:    Free Space
```

Messages

Message 001

```
Date Sent                   05/10/11 20:08:34 TimeZone GMT+0.00H
Sender                      +12404016148
Service Centre              +19703769322
Status                      Message received from Network and read

IEI: 00
LENGTH: 00
MESSAGE REF: 00
STATUS: 01
SC Address length: 07
SC Address type: 91
  Type of number: International
  Numbering plan identifier: E.164
SC Address: 19703769322
Message Type Indicator: 00
Message Type: SMS-DELIVER / SMS-DELIVER REPORT
More Messages To Send: Yes
Status Report Indication: No
Reply Path: No
Originating Address Length: 0B
Originating Address type: 91
  Type of number: International
  Numbering plan identifier: E.164
Originating Address: 12404016148
Protocol Identifier: Default
Data Coding Scheme: GSM Default Alphabet
SC Timestamp: 50011102804300
  decoded: 05/10/11 20:08:34
Time Zone: GMT+0.00H
User Data Length: 13
  decimal: 19
Message: Active incoming sms
```

Fig. 8

3.2.3 Synopsis of ForensicSIM

The ForensicSIM toolkit from Radio Tactics is able to acquire information from SIM cards via a PC/SC-compatible card reader that comes with the software. Before the data contents of the SIM can be analyzed with the Forensic Analysis software, the examiner must use the ForensicSIM acquisition terminal, a stand-alone device, to create a copy of the target SIM on a separate storage card. To copy the SIM, the examiner must log on to the acquisition terminal with a username and PIN number. The acquisition terminal then walks the examiner through the process of entering the target SIM and creating duplicate copies on the provided blank SIM cards (i.e. a Master SIM copy used for storage in case of an evidence dispute, a Prosecution SIM copy that serves as a working duplicate for evidence recovery and analysis and a Defense SIM copy that serves as a working duplicate issued to the defense). In addition to the aforementioned SIM copy cards, Radio Tactics provides the option to create an Access Card. The Access Card holds a copy of data from the target SIM and permits the target handset to be examined without the risk of connecting to the cell network.

Once the target SIM has been successfully duplicated, the ForensicSIM software along with the SIM reader can be used to create a report of the data found on a duplicate working SIM. The ForensicSIM toolkit allows the following data types to be recovered: Subscriber/User related filszses, Phone Number related files, SMS related files, Network related files and General SIM information. Each individual field contains more specific meta-data about each type.

Acquisition Stage

The acquisition process begins by guiding the examiner through a succession of screens about the examination. The examiner has the option of generating a report from either the SIM card or a saved case. As mentioned earlier, the ForensicSIM PC/SC reader is used along with the Radio Tactics ForensicSIM analysis software to acquire data from the SIM card. The initial screen for report and case generation is illustrated below in Fig. 9.

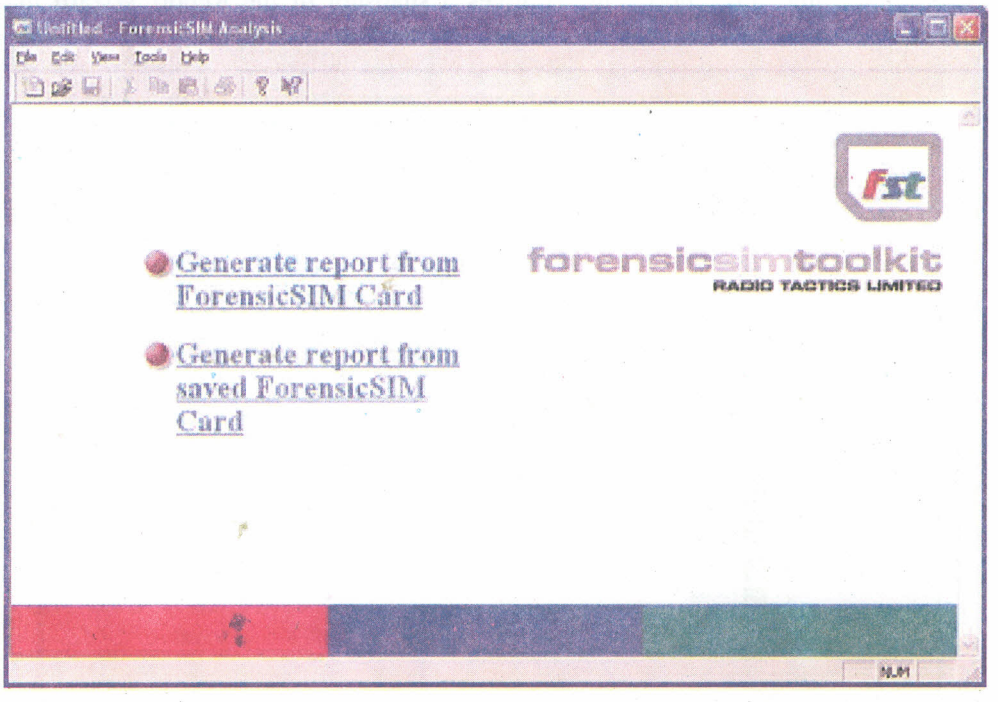


Fig. 9

The examiner has the option of creating a standard report or an advanced report. A standard report displays only card identification information, phonebook and SMS text messages. The advanced report displays additional information recovered from

the SIM card. After the data on the SIM has been successfully acquired, the examiner is then asked to enter case specific information (i.e. Operator, Operator Name, Date/Time, Reference No., Case Reference No., Case Officer, Exhibit Reference, Exhibit Seal No., Exhibit Reseal No., Phone Make, Phone Type, IMEI and PIN/PUK codes, if known). The information entered by the examiner is contained in the finalized report. Illustrated below in Fig. 10 is a snapshot of the User Interface after an acquisition has completed. The user interface provides a tree structure where specific data items can be selected for analysis.

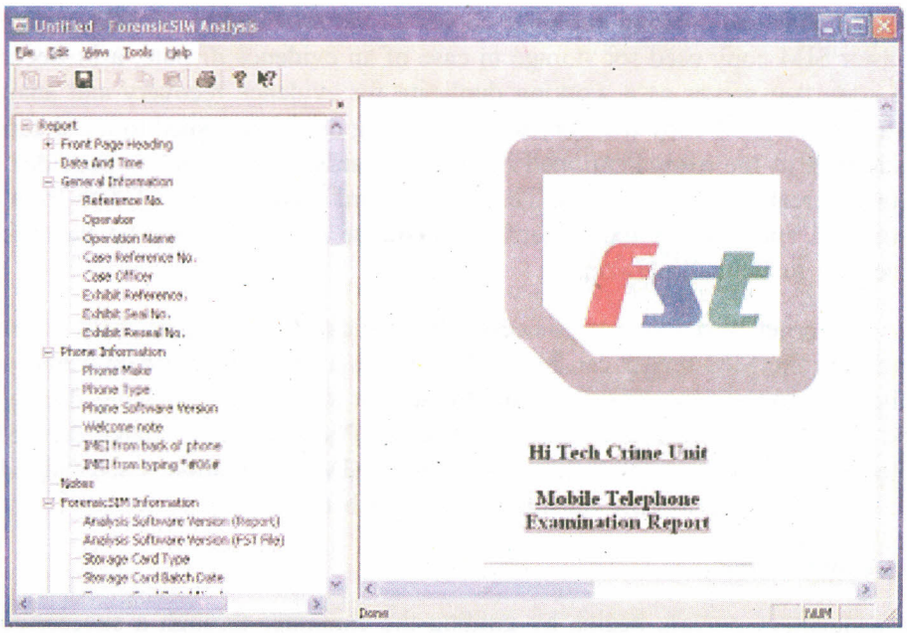


Fig. 10

After a successful acquisition has taken place the examiner then has the opportunity to create a customized report of findings that pertain to the case. To finalize the report, the export option is selected, which allows specific data fields to be incorporated into the report. Fig. 11 gives a snapshot of the Report Wizard that allows examiners to select the data fields for the finalized report.

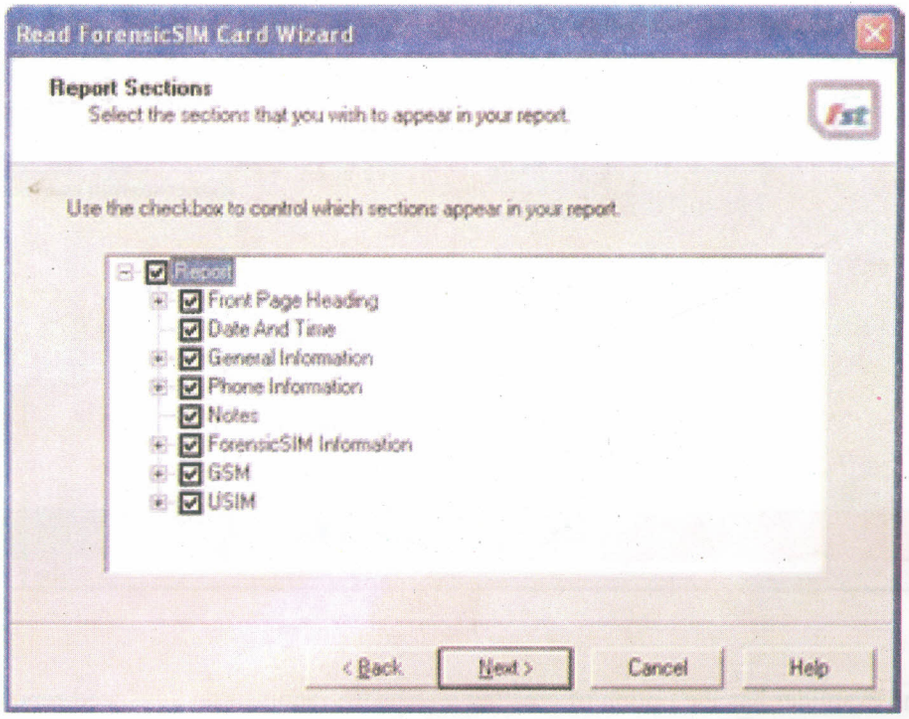


Fig. 11

The examiner has the choice of exporting the final report in the formats illustrated below in Fig. 12.

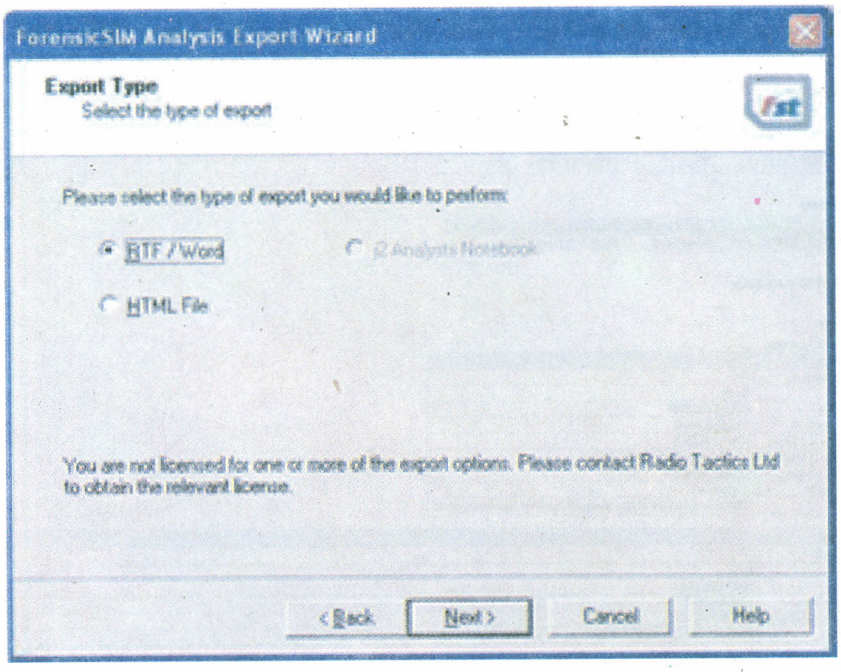


Fig. 12

Fig. 13 are snapshots of the final generated report.

General Information

Reference No.	032805_1
Operator	rpa
Operation Name	richard ayers
Case Reference No.	crn_032805_1
Case Officer	rpa_1
Exhibit Reference.	er_032805_1
Exhibit Seal No.	es_032805_1
Exhibit Reseal No.	ern_032805_1

Phone Information

Phone Make	Nokia
Phone Type	6220
Phone Software Version	Nokia OS

ForensicSIM Information

Analysis Software Version (Report)	1.2.5.0
Analysis Software Version (FST File)	Not present
Storage Card Type	Defence
Storage Card Batch Date	21/06/04
Storage Card Serial Number	0000001732
Storage Card Version	1
Control Card Id	3B6600FF4A434F503130FFFFFFFFFF020065
Control Card User Id	0000
Acquisition Hardware Type	Desktop (MCT5000)
Acquisition Software Version	1.2.1.0
Card Write Start Time	28/03/05 19:39:59
Card Write End Time	Uncalibrated
Number of bytes read	14025
Number of bytes copied	14025
Hash Type	MD5
Hash Code	FCD9A3BBAEF3639C8898C70BED578418

Mobile Station Numbers (MSISDN)

Nr	Name	Telephone Number	Type of number	Numbering Plan	Extension Id
1	MyMobile #	1240731xxxx	International	ISDN/Telephony	None

International Mobile Subscriber Identity (IMSI)

IMSI
310380042199423 MCC: 0310, MNC: 38

Service Provider Name (SPN)

Provider Display Status	Provider Name
Not Displayed	AT&T Wireless

Operator Name String (OPS)

PLMN name
AT&T Wireless

Abbreviated Dialled Numbers

Nr	Name	Telephone Number	Type of number	Numbering Plan	Extension Id
1	[illegible]	9784633210	None	ISDNTelephony	None

Last Number Dialled

Nr	Name	Telephone Number	Type of number	Numbering Plan	Extension Id
1		9784633210	None	ISDNTelephony	None
3		201972xxxx	None	ISDNTelephony	None
4		201973xxxx	None	ISDNTelephony	None

Mailbox Numbers

Nr	Name	Number	Type of number	Numbering Plan	Extension Id
1	Voice Mail	1440200xxxx	International	ISDNTelephony	None

SIM Card SMS Memory Usage

Read messages

There are 2 read messages

SMS Message	
Message Location	1
Status	Read
Message Type	SMS-DELIVER
Originating Address	+12404816148
Service Centre Address	+19703369528
Service Centre Timestamp	25-02-05 10:41:15 GMT -5:00
Data Coding Scheme	Default alphabet
User Data Header	Not present
User Data	This is to determine if sms messages can be properly acquired?

SMS Message	
Message Location	2
Status	Read
Message Type	SMS-DELIVER
Originating Address	12407310023
Service Centre Address	+19703369528
Service Centre Timestamp	09-03-05 16:42:38 GMT +0:00
Data Coding Scheme	Default alphabet
User Data Header	Not present
User Data	ATT Wireless: You received a picture message your phone can't display. See it at the URL below expires soon. Use code dfyrpc2k http://www.attwireless.com/alloc

Fig. 13

3.2.4 Synopsis of Forensic Card Reader

Forensic Card Reader (FCR) version 1.01 is able to acquire information from SIM cards via the PC/SC Chipy reader. The FCR PC/SC USB card reader and FCR software give examiners the ability to capture data such as the ICC ID, IMSI, incoming/outgoing calls, abbreviated call numbers, SMS messages and location data.

Acquisition Stage

After installing the FCR software, connecting the USB reader and selecting the proper PC/SC reader, the SIM data content acquisition begins by clicking the Read button on the beginning wizard screen as illustrated in Fig. 14.

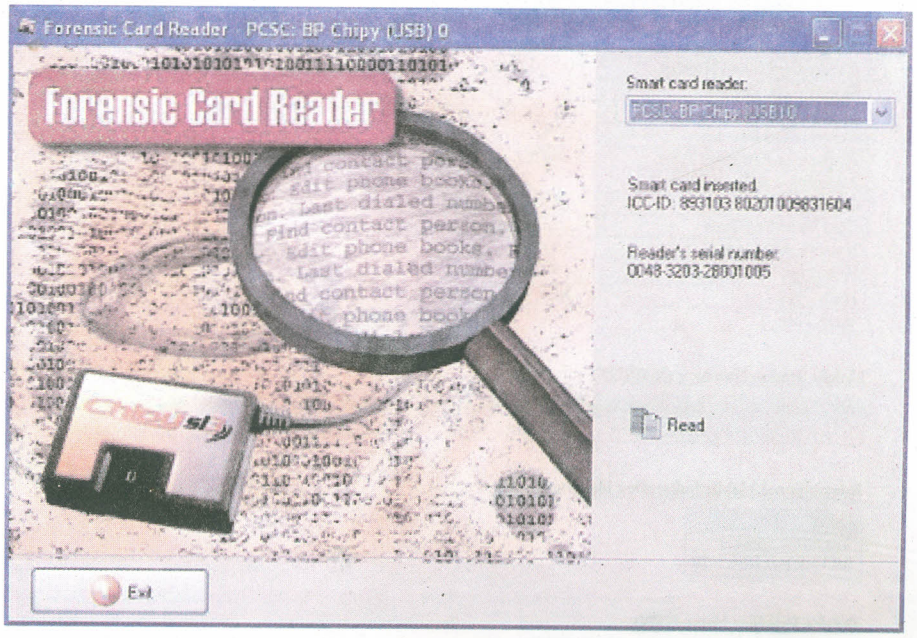


Fig. 14

The wizard allows the examiner to select data elements to be acquired from the SIM and specify the output directory, as illustrated below in Fig. 15.

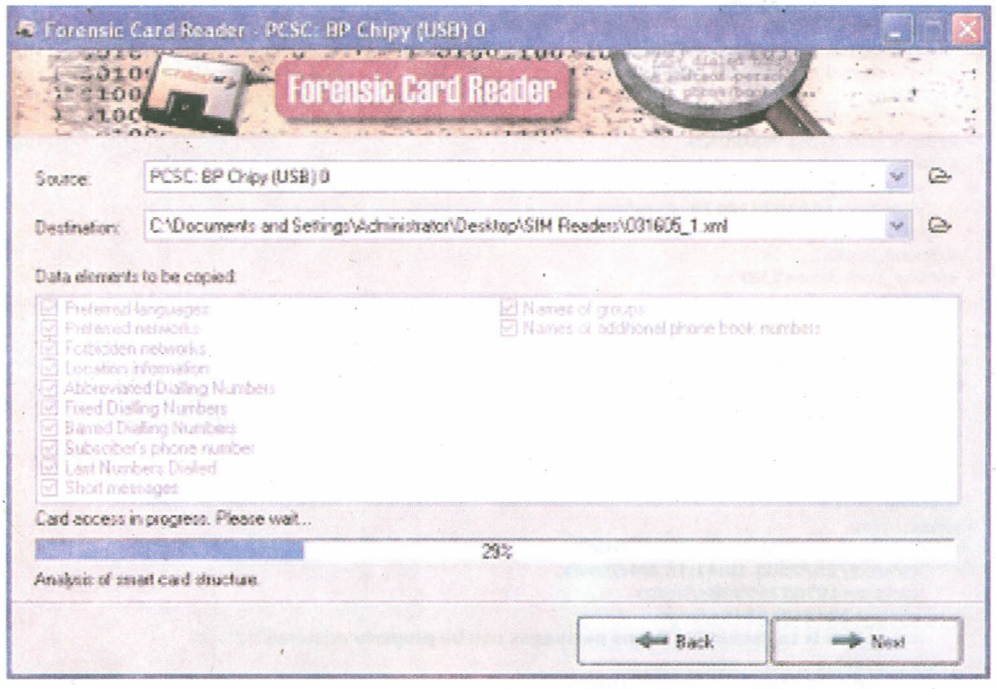


Fig. 15

The acquisition is finalized by clicking the Read button, as illustrated below in Fig. 16. Data elements and acquisition progress are displayed, allowing the progress of the acquisition to be monitored.

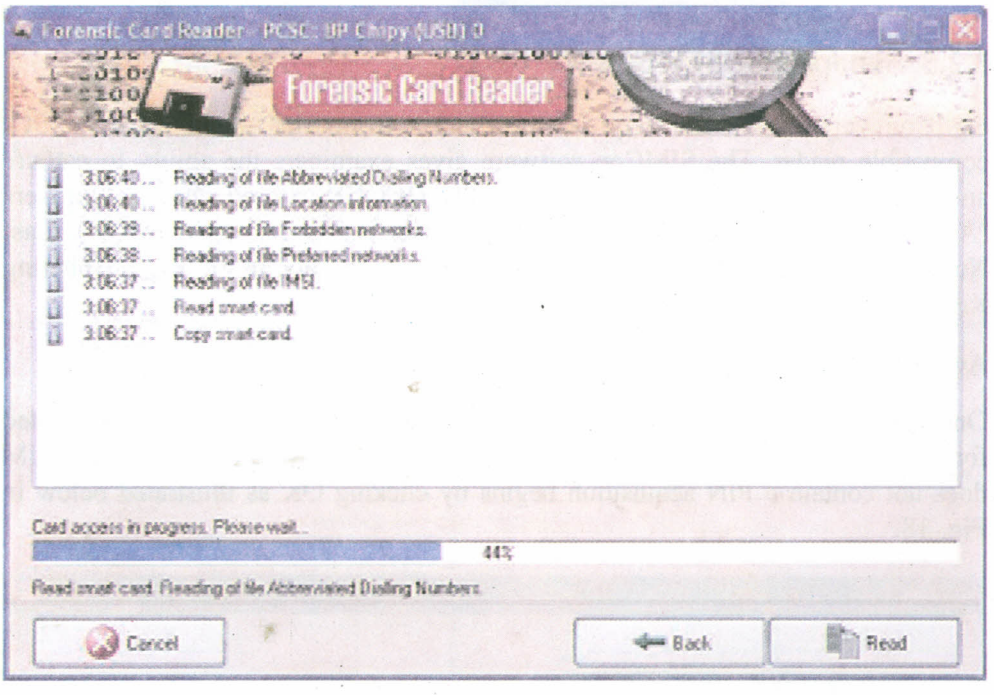


Fig. 16

Report Generation

Once the finalized report is generated, the file can be viewed with an appropriate Web browser or XML editor.

Fig. 17

3.2.5 Synopsis of SIMCon

SIMCon version 1.1 can acquire information from SIM cards via a PC/SC-compatible reader. The SIMCon software gives examiners the ability to capture and examine data such as the Card Identity (ICCID), Stored Dialing Numbers (ADN), Fixed Dialing numbers (FDN), Subscriber Number (MSISDN), Last Numbers Dialed (LND), SMS Messages, Subscriber Identity (IMSI), Ciphering Key (Kc) and Location Information (LOCI).

Acquisition Stage

Once proper connectivity is established with the SIM, the examiner is prompted for the correct PIN, if the SIM is protected, before acquisition begins. If the SIM does not contain a PIN acquisition begins by clicking OK as illustrated below in Fig. 18.

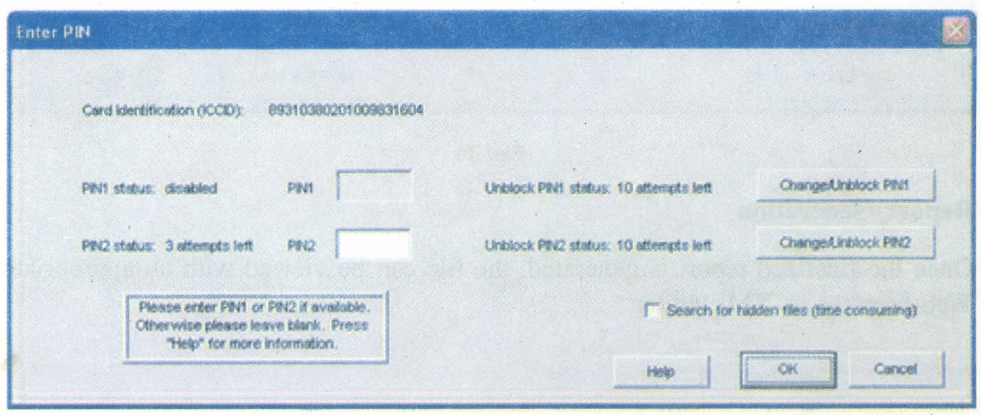


Fig. 18

After a successful acquisition, the entire SIM contents can be saved and stored in the SIMCon .sim proprietary format for later processing. SIMCon allows for examiners to search for hidden files by checking the "Search for hidden files" checkbox, which potentially may uncover pieces of valuable data relevant to the case. SIMCon uses an internal hashing facility to ensure the integrity of cases and detect whether tampering occurred during storage. SIMCon uses the SHA1 algorithm to compute a hash for each file as it is read from the card. Selecting "Verify Hash" in the "File" menu causes SIMCon to recompute all hashes and check that the original file is consistent with the reopened case. Fig. 19 provides a snapshot of the User Interface. The display is divided into three primary panes consisting of a tree structure of data fields, individual data within a selected field and a textual or hexadecimal view of the data selected for investigation.

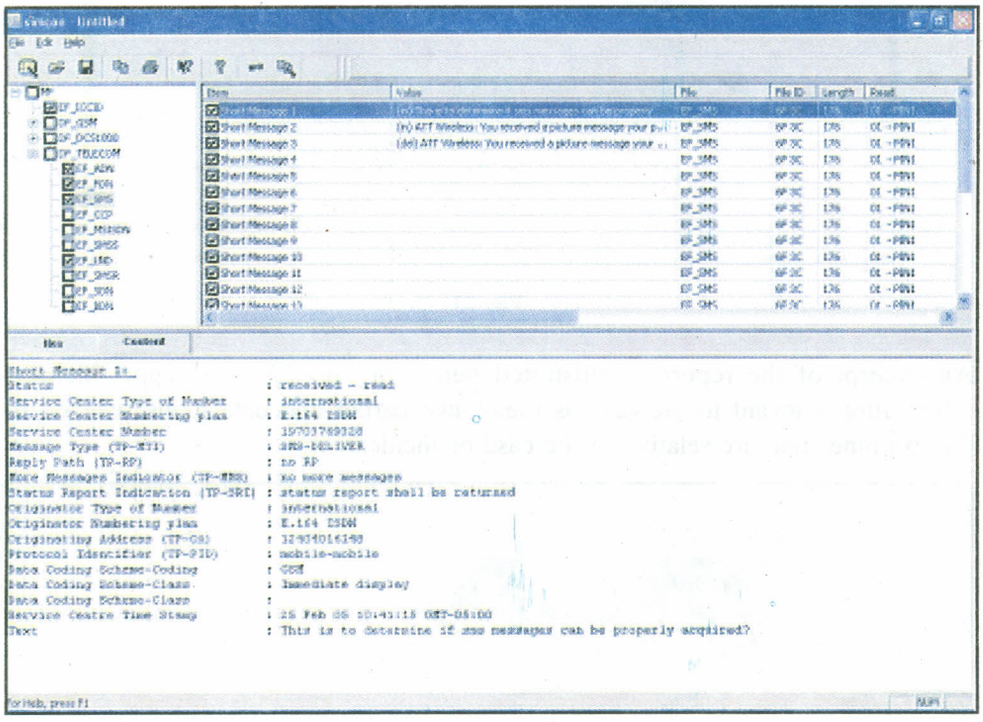


Fig. 19

Report generation begins by prompting the examiner with case specific details such as investigator name, date/time, case id, evidence number and notes specific to the investigation as illustrated below in Fig. 20.

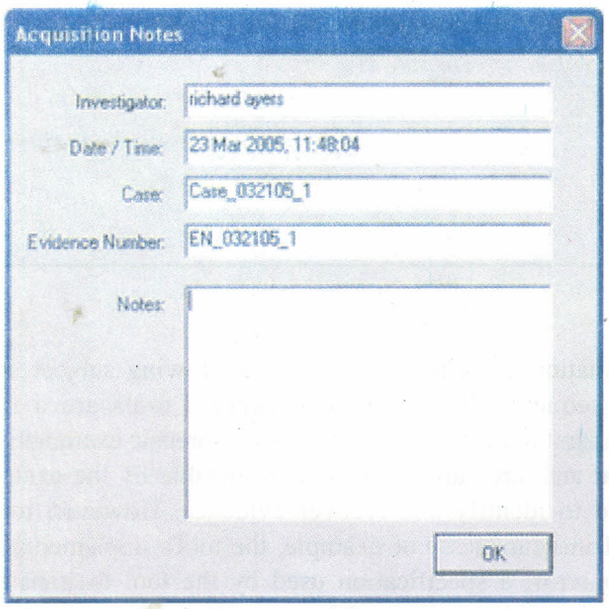


Fig. 20

The final report can either be sent to a printer or saved to a file. As illustrated below in Fig. 21, the examiner can include checked data items, highlighted items or all items in the final report.

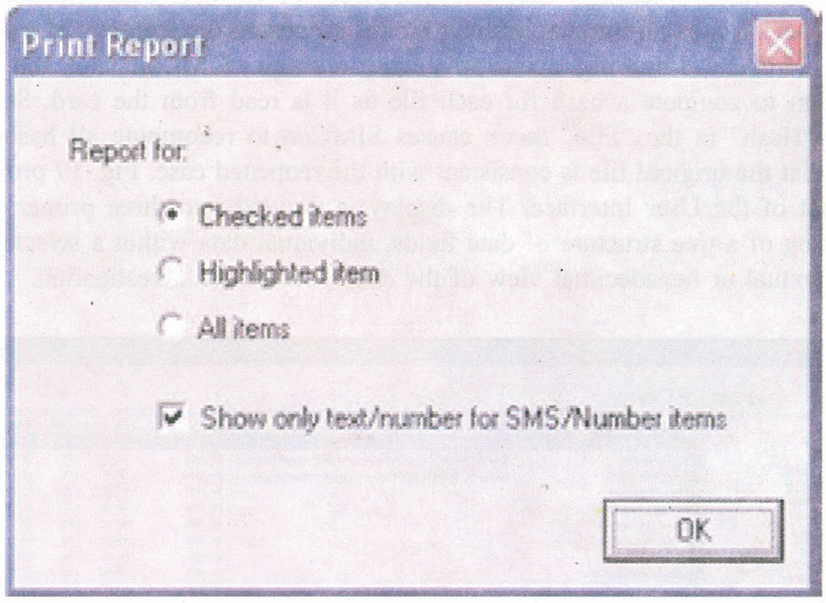


Fig. 21

An excerpt of the report is illustrated below in Fig. 22. The report includes information relevant to the case as mentioned earlier and data items selected by the examiner that are relative to the case or incident.

```
Investigator          : richard ayers
Case                  : case_032105_1
Evidence number       : EN_032105_1
Timestamp             : 23 Mar 2005, 11:40:04
Notes                 :

Card Identity: 89310380201009031604

International Mobile Subscriber Identity (IMSI): 310380042199423 - USA 3650 AT&T, IMEI: 351102/50/2/******

International Mobile Subscriber Identity (IMSI): 310380042199423 - USA 3650 AT&T, IMEI: 351102/50/2/******

Abbreviated Dialling Number 1:
Identifier                    : homer simpson
Type of Number                :
Numbering plan                : E.164 ISDN
Number                        : 9784653210
Capability config id          : FF


Short Message 1:
Status                        : received - read
Service Center Type of Number : International
Service Center Numbering plan : E.164 ISDN
Service Center Number         : 19703780528
Message Type (TP-MTI)         : SMS-DELIVER
Reply Path (TP-RP)            : no RP
More Messages Indicator (TP-MMS) : no more messages
Status Report Indication (TP-SRI) : status report shall be returned
Originator Type of Number     : International
Originator Numbering plan     : E.164 ISDN
Originating Address (TP-OA)   : 12404016148
Protocol Identifier (TP-PID)  : mobile-mobile
Data Coding Scheme-Coding     : GSM
Data Coding Scheme-Class      : Immediate display
Data Coding Scheme-Class      :
Service Centre Time Stamp     : 25 Feb 05 10:41:15 GMT-05:00
Text                          : This is to determine if sms messages can be properly acquire

Last number dialled 1:
Identifier                    :
Type of Number                :
Numbering plan                : E.164 ISDN
Number                        : 9784653210
Capability config id          : FF
```

Fig. 22

Forensic examination of cellular devices is a growing subject area in computer forensics. Consequentially, cell phone forensic tools are a relatively recent development and in the early stages of maturity. Forensic examination tools translate data to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence. However, tools may contain some degree of inaccuracies. For example, the tool's implementation may contain a programming error; a specification used by the tool to translate encoded bits into data comprehensible by the examiner may be inaccurate or out of date; or the

protocol structure generated by the cellular device as input may be incorrect, causing the tool to function improperly. In addition, a knowledgeable suspect may tamper with device information to foil the workings of a tool or apply a wiping tool to remove or eliminate data. Over time, experience with a tool provides an understanding of its limitations, allowing an examiner to compensate where possible for any shortcomings or to turn to other means of recovery.

While the tools discussed have generally performed well and have adequate functionality, new versions are expected to improve and better meet investigative requirements.

3.3 CRITERIA FOR CHOOSING TOOL

The following criteria highlight some items to consider when choosing among available tools:

- Usability – the ability to present data in a form that is useful to an investigator.
- Comprehensive – the ability to present all data to an investigator so that evidence pertaining to an investigation can be identified.
- Accuracy – the quality that the output of the tool has been verified and a margin of error ascertained.
- Deterministic – the ability for the tool to produce the same output when given the same set of instructions and input data.
- Verifiable – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results.
- Acceptance – the degree of peer review and agreement about the methodology or technique used by the tool.
- Quality – the technical support, reliability and maintenance provided by the manufacturer
- Capability – the supported devices, feature set, performance and richness of features with regard to flexibility and customization
- Affordability – the cost versus the associated benefits in productivity

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is ForensicSIM?

.....

.....

.....

.....

.....

.....

.....

.....

3.4 LET US SUM UP

This unit deals with the "Aplications of SIM card reader's". The Synopsis of SIMIS, Synopsis of ForensicSIM, Synopsis of Forensic Card Reader, Synopsis of SIMCon are discussed in detail.

3.5 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

Forensic SIM

The ForensicSIM toolkit from Radio Tactics is able to acquire information from SIM cards via a PC/SC-compatible card reader that comes with the software. Before the data contents of the SIM can be analyzed with the Forensic Analysis software, the examiner must use the ForensicSIM acquisition terminal, a stand-alone device, to create a copy of the target SIM on a separate storage card. To copy the SIM, the examiner must log on to the acquisition terminal with a username and PIN number. The acquisition terminal then walks the examiner through the process of entering the target SIM and creating duplicate copies on the provided blank SIM cards (i.e. a Master SIM copy used for storage in case of an evidence dispute, a Prosecution SIM copy that serves as a working duplicate for evidence recovery and analysis and a Defense SIM copy that serves as a working duplicate issued to the defense). In addition to the aforementioned SIM copy cards, Radio Tactics provides the option to create an Access Card. The Access Card holds a copy of data from the target SIM and permits the target handset to be examined without the risk of connecting to the cell network.

UNIT 4 FORENSIC EXAMINATION OF MOBILE DEVICES

Structure

4.0 INTRODUCTION

The variety of forensic toolkits for cell phones and other handheld devices is diverse. A considerable number of software tools and toolkits exist, but the range of devices over which they operate is typically narrowed to distinct platforms for a manufacturer's product line, a family of operating systems, or a type of hardware architecture. Moreover, the tools require that the examiner have full access to the device (i.e. the device is not protected by some authentication mechanism or the examiner can satisfy any authentication mechanism encountered).

4.1 OBJECTIVES

After going through this Unit, you should be able to:

- elucidate various tools used in forensic examination of mobile; and
- analyze various tools used in forensic examination of mobile devices.

4.2 FORENSIC EXAMINATION OF MOBILE DEVICES

While most toolkits support a full range of acquisition, examination, and reporting functions, some tools focus on a subset. Similarly, different tools may be capable of using different interfaces (e.g. IrDA, Bluetooth, or serial cable) to acquire device contents. The types of information that tool can acquire can range widely and include PIM (Personal Information Management) data (e.g. phone book); logs of phone calls; SMS/EMS/MMS messages, e-mail, and IM content; URLs and content of visited Web sites; audio, video, and image content; SIM content; and uninterrupted image data. Information present on a cell phone can vary depending on several factors, including the following:

- The inherent capabilities of the phone implemented by the manufacturer
- The modifications made to the phone by the service provider or network operator
- The network services subscribed to and used by the user
- The modifications made to the phone by the user

Acquisition through a cable interface generally yields superior acquisition results than other device interfaces. However, a wireless interface such as infrared or Bluetooth can serve as a reasonable alternative when the correct cable is not readily

available. Regardless of the interface used, one must be vigilant about any forensic issues associated. Note too that the ability to acquire the contents of a resident SIM may not be supported by some tools, particularly those strongly oriented toward PDAs. Table 1 lists open-source and commercially available tools and the facilities they provide for certain types of cell phones.

Table 1: Cell Phone Tools

	Function	Feature
PDA Seizure	Acquisition, Examination, Reporting	• Targets Palm OS, Pocket PC, and RIM OS phones • No support for recovering SIM information • Supports only cable interface
Pilot Link	Acquisition	• Targets Palm OS phones • Open source non-forensic software • No support for recovering SIM information • Supports only cable interface
Cell Seizure	Acquisition, Examination, Reporting	• Targets certain models of GSM, TDMA, and CDMA phones • Supports recovery of internal and external SIM • Supports only cable interface
GSM .XRY	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Supports recovery of internal and external SIM • Supports cable, Bluetooth, and IR interfaces
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Supports only internal SIM acquisition
MOBILedit! Forensic	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Internal and external SIM support • Supports cable and IR interfaces
BitPIM	Acquisition, Examination	• Targets certain models of CDMA phones • Open source software with write-blocking capabilities • No support for recovering SIM information
TULP 2G	Acquisition, Reporting	• Targets GSM and CDMA phones that use the supported protocols to establish connectivity • Internal and external SIM support • Requires PC/SC-compatible smart card reader for external SIM cards • Cable, Bluetooth, and IR interfaces supported

Because of the way GSM phones are logically and physically partitioned into a handset and SIM, a number of forensic software tools have emerged that deal exclusively with SIMs independently of their handsets. The SIM must be removed from the phone and inserted into an appropriate reader for acquisition. SIM forensic tools require either a specialized reader that accepts a SIM directly or a general-purpose reader for a full-size smart card. For the latter, a standard-size smart card adapter is needed to house the SIM for use with the reader. Table 2 lists several SIM forensic tools. The first four listed, Cell Seizure, TULP2G, GSM .XRY, and Mobiledit!, also handle phone memory acquisition, as noted above.

Table 2: SIM Tools

Cell Seizure	Acquisition, Examination, Reporting	• Also recover information from SIM card, when inserted in handset
TULP 2G	Acquisition, Reporting	• Also recover information from SIM card, when inserted in handset
GSM .XRY	Acquisition, Examination, Reporting	• Also recover information from SIM card, when inserted in handset
Mobiledit! Forensic	Acquisition, Examination, Reporting	• Also recover information from SIM card, when inserted in handset
SIMIS	Acquisition, Examination, Reporting	• External SIM cards only
ForensicSIM	Acquisition, Examination, Reporting	• External SIM cards only • Produces physical facsimiles of SIM for prosecutor and defense, and as a storage record
Forensic Card Reader	Acquisition, Reporting	• External SIM cards only
SIMCon	Acquisition, Examination, Reporting	• External SIM cards only

Forensic software tools acquire data from a device in one of two ways: physical acquisition or logical acquisition. Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g. a disk drive or RAM chip), while logical acquisition implies a bit-by-bit copy of logical storage objects (e.g. directories and files) that reside on a logical store. The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e. a logical view), versus memory as seen by the processor and other hardware components (i.e. a physical view). In general, physical acquisition is preferable, since it allows any data remnants present (e.g. unallocated RAM or unused filesystem space) to be examined, which otherwise would go unaccounted in a logical acquisition. Physical device images are generally more easily imported into another tool for examination and reporting. However, a logical acquisition provides a more natural and understandable organization of the information acquired. Thus, if possible, doing both types of acquisition is preferable.

Tools not designed specifically for forensic purposes are questionable and should be thoroughly evaluated before use. Though both forensic and non-forensic software

tools generally use the same protocols to communicate with the device, non-forensic tools allow a two-way flow of information in order to populate and manage the device, and avoid taking hashes of acquired content for integrity purposes. Documentation also may be limited and source code unavailable for examination, respectively increasing the likelihood of error and decreasing confidence in the results. On the one hand, non-forensic tools might be the only means to retrieve information that could be relevant as evidence. On the other, they might overwrite, append, or otherwise cause information to be lost, if not used carefully.

PDA Seizure

Paraben's PDA Seizure version 3.0.3.89 is a forensic software toolkit that allows forensic examiners to acquire, search, examine, and report data associated with PDAs running Palm OS, Windows CE, and RIM OS. Though able to be used with smart phones running these operating systems, the toolkit is oriented toward non-cellular devices and omits cell phone-oriented features, such as SIM acquisition for GSM phones. PDA Seizure's features include the ability to perform a logical and physical acquisition, providing a view of internal memory and relevant information concerning individual files and databases. PDA Seizure uses the MD5 hash function to protect the integrity of acquired files. Additional features include bookmarking of information to be filtered and organized in a report format, searching for text strings within the acquired data, and automatic assembly found images under a single facility.

Pilot-Link

Pilot-link is an open source software suite originally developed for the Linux community to allow information to be transferred between Linux hosts and Palm OS devices. It runs on several other desktop operating systems besides Linux, including Windows and Mac OS. About thirty command line programs comprise the software suite. To perform a physical and logical dump, pilot-link establishes a connection to the device with the aid of the Hotsync protocol. The two programs of interest to forensic examiners are pi-getram and pi-getrom, which respectively retrieve the physical contents of RAM and ROM from a device. Another useful program is pilot-xfer, which allows the installation of programs and the backup and restoration of databases. pilot-xfer provides a means to acquire the contents of a device logically. The contents retrieved with these utilities can be manually examined with either the Palm OS Emulator (POSE), a compatible forensics tool such as EnCase, or a hex editor. pilot-link does not provide hash values of the information acquired. A separate step must be carried out to obtain needed hash values.

Cell Seizure

Paraben's Cell Seizure version 2.0.0.33660 is a forensic software toolkit that allows forensic examiners to acquire, search, examine, and report data associated with cell phones operating over CDMA, TDMA, and GSM networks. To acquire data from cell phones using Paraben's Cell Seizure software, the proper cable must be selected from either the Cell Seizure Toolbox or a compatible cable (e.g. datapilot) to establish a data-link between the phone and the forensic workstation. The type of phone being acquired determines the cable interface. Serial RS-232 and USB data-link connections are established via the phone data port or the under-battery interface connection. Additional features include bookmarking of information to be filtered and organized in a format report, searching for case-sensitive whole word text and hexadecimal values, and automatic assembly of found images under a single facility. The following data can usually be found on most cell phones with the tool:

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

GSM .XRY

Micro Systemation's SoftGSM .XRY is a forensic software toolkit for acquiring data from GSM, CDMA, 3G phones and SIM/USIM cards. The .XRY unit is able to connect to cell phone devices via Infrared (IR) port, Bluetooth or a cable interface. After establishing connectivity, the phone model is identified with a corresponding picture of the phone, the device name, manufacturer, model, serial number (IMEI), Subscriber ID (IMSI), manufacturer code, device clock, and the PC clock. Data acquired from cell phone devices are stored in the .XRY format and cannot be altered, but can be exported into external formats and viewed with third-party applications. After a successful acquisition, the following fields may be populated with data, depending on the phone's functionality: Summary screen, Case data, General Information, Contacts, Calls, Calendar, SMS, Pictures, Audio, Files, Notes, Tasks, MMS, Network Information, Video, etc. Additionally, graphic files, audio files, and internal files present on the phone can be viewed internally or exported to the forensic workstation for safekeeping or further investigation.

Oxygen Phone Manager

The forensic version of Oxygen Phone Manager is available for Police Departments, Law Enforcement units, and all government services that wish to use the software for investigation purposes. The forensic version differs from the non-forensic version of Oxygen Phone Manager by prohibiting any changes in data during acquisition. Oxygen Phone Manager (OPM) allows examiners to acquire data from the device and export the acquired data into multiple supported formats. The Oxygen software is tailored toward mobile phones and smart phones manufactured by: Nokia, Sony Ericsson, Siemens, Panasonic, Sendo, BenQ and some Samsung models. Oxygen software provides software libraries, ActiveX libraries and components for Borland Delphi to software developers.

MOBILedit!

MOBILedit! Forensic is an application giving examiners the ability to acquire logically, search, examine and report data from GSM/CDMA/PCS cell phone devices. MOBILedit! is able to connect to cell phone devices via an Infrared (IR) port, a Bluetooth link, or a cable interface. After connectivity has been established, the phone model is identified by its manufacturer, model number, and serial number (IMEI) and with a corresponding picture of the phone. Data acquired from cell phone devices are stored in the .med file format. After a successful acquisition, the following fields are populated with data: subscriber information, device specifics, Phonebook, SIM Phonebook, Missed Calls, Last Numbers Dialed, Received Calls, Inbox, Sent Items, Drafts, Files folder. Items present in the Files folder, ranging from Graphics files to Camera Photos and Tones, depend on the phone's capabilities. Additional features include the myPhoneSafe.com service, which provides access to the IMEI database to register and check for stolen phones.

BitPIM

BitPIM is a phone management program that runs on Windows, Linux and Mac OS and allows the viewing and manipulation of data on cell phones. This data includes the phone book, calendar, wallpapers, ring tones and the embedded filesystem. To acquire data successfully using BitPIM, examiners must have the proper driver and cable to form a connection between the phone and the forensic workstation. BitPIM provides detailed information contained in the help file, outlining supported phones, suggested cables to use with specific phone models, and notes and How-Tos about specific situations. BitPIM is distributed as open source software under the GNU General Public License.

TULP 2G

TULP2G (2nd generation) is an open source, forensic software tool originated by the Netherlands Forensic Institute that allows examiners to extract and read data from mobile cell phones and SIMs. TULP2G requires a forensic workstation running either Windows 2000 or XP, preferably with the latest patches and service pack installed, along with .NET 1.1 SP1. In order to take advantage of newly released 1.1 plug-ins, Windows XP SP2 is required. TULP2G acquires data from mobile phones using a proper data cable, Bluetooth or IrDA connection and a compatible protocol plug-in. Reading SIMs requires a PC/SC-compatible smart card reader and possibly an adapter to convert a small-sized SIM to the standard-size smart card format.

SIMIS

SIMIS is a forensic tool from Crownhill USA that allows examiners the ability to extract data from a SIM securely and protect the integrity with cryptographic hashes. A USB dongle is needed to operate the software on a desktop computer. The SIMIS desktop is capable of decoding unicode data found on the SIM Card, including active and deleted text messages and phone book information. The company also offers the SIMIS Mobile Handheld Reader, which is a portable stand-alone SIM reader that can capture SIM data for transfer to the SIMIS desktop.

ForensicSIM

Radio Tactic's ForensicSIM Toolkit consists of the following components: acquisition terminal, control card, data storage cards, analysis application, and the card reader. The acquisition terminal is a stand-alone unit that guides the examiner through each step of the acquisition process. The ForensicSIM toolkit deals with two processes: acquisition of data and analysis of data. Data acquisition is carried out using the acquisition terminal. Data analysis is carried out using the ForensicSIM card reader, attached to a PC running the ForensicSIM analysis application. The terminal's primary function is to capture copies of the data from the target SIM to a set of data storage cards. A control card is used to provide the examiner access to the acquisition terminal, thwarting unauthorized use. The data storage cards consist of a master data storage card, a prosecution data storage card, a defense data storage card, and a handset access card. The toolkit allows examiners read-only access to SIMs and generates textual reports based on the contents acquired. Reports can be viewed internally, saved to disk, or printed for presentation purposes.

Forensic Card Reader

The Forensic Card Reader (FCR) consists of a smart card reader with USB connection and the FCR software that gives examiners the ability to acquire data from SIM cards without modification. The examiner has the ability to select specific data elements that can be later stored and displayed in a finalized report. Operations details like case number, evidence number, and examiner can be automatically merged into the report and its file name. All usual data elements are acquired (e.g. phone directory, abbreviated dialing numbers, fixed dialing numbers and SMS messages), as well as the identifiers of the SIM and the subscriber. Special elements

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

SIMCon

SIMCon works with any standard smart card reader compliant with the PC/SC standard. Upon completing the acquisition of the SIM card data, SIMCon card content is stored in unique files identified by a two-byte File ID code. Individual files may contain many informative elements called "items" and are displayed in tabular form. Each item, when selected, can be shown in hexadecimal or a textual interpretation. Besides standard SIM file content, SIMCon also has an option to do a comprehensive scan of all directories and files that may be present on the SIM, to acquire non-standardized directories and files. Examiners can create customized reports by selecting file information that pertains to the investigation.

4.3 ANALYSIS OVERVIEW

A simple methodology was followed to understand and gauge the capabilities of the forensic tools described in the previous section. The main steps are illustrated in Fig. 1. First, a set of target devices ranging from simple to smart phones was assembled. Then, a set of prescribed activities, such as placing and receiving calls, was performed for each phone. After each such scenario, the contents of the phone and/or associated SIM were acquired using an available tool and examined to see if the results of an activity could be recovered as expected. Finally, an assignment was made about how well the tool met predefined expectations. The process was repeated for each scenario defined. At least two different individuals performed each scenario and assigned a rating separately; any noted inconsistencies were resolved.

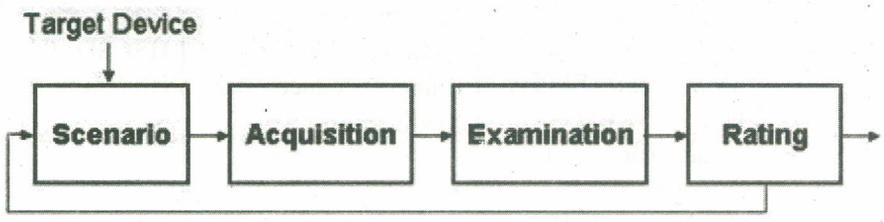


Fig. 1: Tool Assessment

For GSM phones, two sets of scenarios were applied: one for handsets containing an associated SIM, and the other for SIMs removed from their handsets and examined independently. For CDMA and other types of phones that do not depend on a SIM, only the former set was used.

4.4 TARGET DEVICES

A suitable but limited number of target devices were needed on which to conduct the scenarios. The target devices selected, while not extensive, cover a range of operating systems, processor types, and hardware components. These variations were intended to uncover subtle differences in the behavior of the forensic tools in acquisition and examination. Table 3 highlights the key characteristics of each target device, listed roughly from devices with more capabilities to less-capable devices, rather than alphabetically. Note that the more capable devices listed have a PDA heritage, insofar as they use Windows Mobile, Palm OS, RIM OS, and Symbian operating systems.

Table 3

	Software	Hardware	Wireless
Motorola MPX220	Windows Mobile for Smart phones 2003 SMS, EMS, MMS SMS Chat Email (IMAP4, POP3) Web (HTML, WAP 2.0)	200 MHz OMAP 1611 processor 64 MB ROM 32 MB RAM Color display 2nd monochrome display Camera MiniSD slot	GSM 850/900/ 1800/1900 GPRS Bluetooth IrDA
Treo 600	Palm OS 5.2 SMS, EMS, MMS SMS Chat Email (POP3, SMTP) Web (HTML 4.0, XHTML, WML 1.3)	144 MHz OMAP 1510 ARM-based processor 32 megs of RAM (24 MB vailable) Color display QUERTY keypad SD/MMC slot (with SDIO)	GSM 850/900/ 1800/1900 GPRS IrDA
Sony Ericsson P910a	Symbian 7.0, UIQ 2.1 SMS, EMS, MMS Email (POP3, IMAP4) Web (WAP)	ARM 9 processor 64MB ROM 32MB RAM Color display Camera Memory Stick duo pro slot	GSM 850/ 1800/1900 HSCSD, GPRS Bluetooth IrDA
Samsung i700	Pocket PC 2002 Phone Edition SMS (no EMS/MMS) Email Web Instant Messaging	300 MHz StrongArm PXA250 processor 32MB flash memory 64MB SDRAM Color display Swivel camera SD/MMC slot (with SDIO)	AMPS 800 CDMA 800/ 1900 1xRTT IrDA
Nokia 7610	Symbian 7.0, Series 60 2.0 SMS, MMSConcatenated SMS Email (SMTP, POP3, IMAP4) Instant Messaging Web (WAP 2.0, HTML, XHTML and WML)	123 MHz processor 8 MB internal dynamic memory Color display Camera Reduced Size MMC slot	GSM 850/ 1800/1900 HSCSD, GPRS Bluetooth
Kyocera 7135	Palm OS 4.1 SMS, EMS (no MMS) Email (POP, IMAP, SMTP) Web (HTML 3.2)	33 MHz Dragonball VZ processor 16 MB volatile Color Display SD/MMC slot (with SDIO)	AMPS 800 CDMA 800/ 1900 1xRTT IrDA
BlackBerry 7780	RIM OS SMS Email (POP3) Web (WAP)	16 MB flash memory plus 2 MB SRAM Color display QWERTY keypad	GSM 850/ 1800/1900 GPRS
BlackBerry 7750	RIM OS SMS (no EMS/SMS) Email (POP3, IMAP4) Web (WAP 2.0, WML/ HTML)	ARM7TDMI (Qualcomm 5100 Chipset) 14 MB flash memory 2 MB SRAM Color display QWERTY keypad	CDMA 800/ 1900 1xRTT

Motorola V300	SMS, EMS, MS SMS Chat Nokia Smart Message Instant Messaging Email (SMTP, POP3, IMAP4) Web (WAP 2.0)	Internal Memory 5MB Color display Camera	GSM 900/1800/ 1900 GPRS
Nokia 6610i	Series 40 SMS, MMS Concatenated SMS SMS Chat No Email Web (WAP 1.2.1 XHTML)	4 MB user memory 8-line color display Camera	GSM 900/1800/ 1900 HSCSD, GPRS IrDA
Ericsson T68i	SMS/EMS messaging MMS messaging Email (POP3,SMTP) SMS Chat Web (WAP 1.2.1/2.0, WLTS)	FM radio Color display Optional camera attachment	GSM 900/1800/ 1900 HSCSD, GPRS Bluetooth IrDA
Sanyo 8200	SMS, EMS Picture Mail Email Web WAP 2.0 Mobile-to-mobile (walkie talkie)	Color display 2nd color display Camera	AMPS 850 CDMA 850/ 1900
Nokia 6200	SMS, EMS, MMS Email over SMS SMS Chat Web (WAP 1.2.1, XHTML)	Color display FM radio	GSM 850/1800/ 1900 GPRS, EDGE IrDA
Audiovox 8910	EMS, MMS SMS Chat No email Web (WAP 2.0)	Color display2nd monochrome display Camera	AMPS 850 CDMA800/1900 1xRTT
Motorola C333	SMS, EMS SMS chat WAP 1.2.1	Monochrome graphic display	GSM 850/1900 GPRS
Motorola V66	SMS (no EMS) AOL Instant Messenger Web (WAP 1.1)	Monochrome graphic display	GSM 900/1800/ 1900 GPRS
Nokia 3390	SMS Picture messaging Email over SMS AOL Instant Messaging	Monochrome graphic display	GSM 1900

Every tool does not support every target device. In fact, the opposite is true – a specific tool typically supports only a limited number of devices. The determination of which tool to use for which device was based primarily on the tool's documented list of supported phones. Whenever ambiguity existed, an acquisition attempt was conducted to make a determination. Table 4 summarizes the various target devices used with each tool. The order of the devices bears no relevance on capabilities they are alphabetized for consistency throughout the remaining portion of the document. The table excludes forensic SIM tools, which support most SIMs found in GSM devices.

Table 4

	PDA Seizure	Pilot-link	Cell Seizure	GSM .XRY	OPM	MOBILedit!	TULP 2G	BITpim
Audio Vox								X
Blackberry 7750/ 7780	X							
Ericsson T78i			X	X		X	X	
Kyocera 7135	X	X						
Motorola C333			X			X	X	
Motorola MPX220	X							
Motorola V66			X	X		X	X	
Motorola V300				X	X	X	X	
Nokia 33990			X	X	X		X	
Nokia 6610i			X	X	X	X	X	
Nokia 6200				X	X			
Nokia 7610								
Samsung i700	X							
Sanyo 8200								X

Though SIMs are highly standardized, their content can vary among network operators and service providers. For example, a network operator might create an additional file on the SIM for use in its operations or might install an application to provide a unique service. SIMs may also be classified according to the "phase" of the GSM standards that they support. The three phases defined are phase 1, phase 2, and phase 2+, which correspond roughly to first, second, and 2.5 generation network facilities. Another class of SIMs in early deployment is Universal SIMs (USIMS) used in third generation (3G) networks. Table 5 lists the identifier and phase of the SIMs used in the analysis, the associated network operator, and some of the associated network services activated on the SIM. Except for pay-as-you-go phones, each GSM phone was matched with a SIM that offered services compatible with the phone's capabilities.

Table 5

SIM	Phase	Network	Services
1604	2 - profile download required	AT&T	Abbreviated Dialing Numbers (ADN) Fixed Dialing Numbers (FDN) Short Message Storage (SMS) Last Numbers Dialed (LND) Group Identifier Level 1 (GID1) Group Identifier Level 2 (GID2) Service Dialing Numbers (SDN) General Packet Radio Service (GPRS)
1144	2 - profile download required	AT&T	Abbreviated Dialing Numbers (ADN) Fixed Dialing Numbers (FDN) Short Message Storage (SMS) Last Numbers Dialed (LND) General Packet Radio Service (GPRS)
8778	2 - profile download required	Cingular	Abbreviated Dialing Numbers (ADN) Fixed Dialing Numbers (FDN) Short Message Storage (SMS) Last Numbers Dialed (LND) Group Identifier Level 1 (GID1) Group Identifier Level 2 (GID2) Service Dialing Numbers (SDN) General Packet Radio Service (GPRS)
7202	2 - profile download required	T-Mobile	Abbreviated Dialing Numbers (ADN) Fixed Dialing Numbers (FDN) Short Message Storage (SMS) Last Numbers Dialed (LND) Group Identifier Level 1 (GID1) General Packet Radio Service (GPRS)
5343	2 - profile download required	T-Mobile	Abbreviated Dialing Numbers (ADN) Fixed Dialing Numbers (FDN) Short Message Storage (SMS) Last Numbers Dialed (LND) General Packet Radio Service (GPRS)

Overall, SIM forensic tools do not recover every possible item on a SIM. The breadth of coverage also varies considerably among tools. Table entries give an overview of those items recovered, listed at the left, by the various SIM forensic tools, listed across the top.

Table 6

	Cell Seizure	GSM .XRY	MOBILedit!	TULP 2G	FCR	Forensic SIM	SIMcon	SIMIS
International Mobile Subscriber Identity - IMSI	X	X	X	X	X	X	X	X
Integrated Circuit Card Identifier - ICCID	X	X	X	X	X	X	X	X
Mobile Subscriber ISDN -- MSISDN	X	X		X	X	X	X	X

Service Provider Name - SPN	X			X		X X	X	X X
Phase identification - Phase	X	X	X			X	X	X
SIM Service Table - SST				X		X	X	X
Language Preference - LP	X			X		X	X	X
Abbreviated Dialling Numbrs - AND	X	X	X	X	X	X	X	X
Last numbers dialled - LND	X	X	X	X	X	X X	X	X
Short Message Service SMS	X	X	X	X	X		X	X
Read/ Unread Deleted	X	X		X			X	

A subset of the SIMs used for the phone scenarios were used in the SIM scenarios.

Scenarios

The scenarios define a set of prescribed activities used to gauge the capabilities of the forensic tool to recover information from a phone, beginning with connectivity and acquisition and moving progressively toward more interesting situations involving common applications, file formats, and device settings. The scenarios are not intended to be exhaustive or to serve as a formal product evaluation. However, they attempt to cover a range of situations commonly encountered when examining a device (e.g. data obfuscation, data hiding, data purging) and are useful in determining the features and functionality afforded an examiner.

Table below gives an overview of these scenarios, which are generic to all devices that have cellular phone capabilities. For each scenario listed, a description of its purpose, method of execution, and expected results are summarized. Note that the expectations are comparable to those an examiner would have when dealing with the contents of a hard disk drive as opposed to a PDA/cell phone. Though the characteristics of the two are quite different, the recovery and analysis of information from a hard drive is a well-understood baseline for comparison and pedagogical purposes. Moreover, comparable means of digital evidence recovery from most phones exists, such as desoldering and removing non-volatile memory and reading out the contents with a suitable device programmer. Also note that none of the scenarios attempt to confirm whether the integrity of the data on a device is preserved when applying a tool – that topic is outside the scope of this document.

Table 7

Scenario	Description
Connectivity and Retrieval	Determine if the tool can successfully connect to the device and retrieve content from it. • Enable user authentication on the device before acquisition, requiring a PIN, password, or other known authentication information to be supplied for access. • Initiate the tool on a forensic workstation, attempt to connect with the device and acquire its contents, verify that the results are consistent with the known characteristics of the device. • Expect that the authentication mechanism(s) can be satisfied without affecting the tool, and information residing on the device can be retrieved.
PIM Applications	Determine whether the tool can find information, including deleted information, associated with Personal Information Management (PIM) applications such as phone book and date book. • Create various types of PIM files on the device, selectively delete some entries, acquire the contents of the device, locate and display the information. • Expect that all PIM-related information on the device can be found and reported, if not previously deleted. Expect that remnants of deleted information can be recovered and reported.
Dialled/Received Phone Calls	Determine whether the tool can find dialed and received phone calls, including unanswered and deleted calls. • Place and receive various calls to and from different numbers, selectively delete some entries, acquire the contents of the device, locate and display dialled and received calls. • Expect that all dialled and received phone calls on the device can be recognized and reported, if not previously deleted. Expect that remnants of deleted information can be recovered and reported.
SMS/MMS Messaging	Determine whether the tool can find placed and received SMS/MMS messages, including deleted messages. • Place and receive both SMS and MMS messages, selectively delete some messages, acquire the contents of the device, locate and display all messages. • Expect that all sent and received SMS/MMS messages on the device can be recognized and reported, if not previously deleted. Expect that remnants of deleted information can be recovered and reported.

Scenario	Description
Internet Messaging	Determine whether the tool can find sent and received e-mail and Instant Message (IM) messages, including deleted messages. • Send and receive both IM and e-mail messages, selectively delete some messages, acquire the contents of the device, locate and display all messages. • Expect that all sent and received IM and messages on the device can be recognized and reported, if not previously deleted. Expect that remnants of deleted information can be recovered and reported.
Web Applications	Determine whether the tool can find a visited Web site and information exchanged over the internet. • Use the device to visit specific Web sites and perform queries, acquire the contents of the device, selectively delete some data, locate and display the URLs of visited sites and any associated data acquired (e.g. images, text, etc.). • Expect that information about most recent Web activity can be found and reported.
Text File Formats	Determine whether the tool can find and display a compilation of text files residing on the device, including deleted files. • Load the device with various types of text files, (via e-mail and device synchronization protocols), selectively delete some files, acquire the contents of the device, find and report the data. • Expect that all files with common text file formats (i.e. .txt, .doc, .pdf) can be found and reported, if not deleted. Expect that remnants of deleted information can be recovered and reported.
Graphics File Formats	Determine whether the tool can find and display a compilation of the graphics formatted files residing on the device, including deleted files. • Load the device with various types of graphics files, (via e-mail and device synchronization protocols) selectively delete some files, acquire the contents of the device, locate and display the images. • Expect that all files with common graphics files formats (i.e. .bmp, .jpg, .gif, .tif, and .png) can be found, reported, and collectively displayed, if not deleted. Expect that remnants of deleted information can be recovered and reported.
Compressed Archive File Formats	Determine whether the tool can find text, images, and other information located within compressed-archive formatted files (i.e. .zip, .rar, .tar, .tgz, and self-extracting .exe) residing on the device. • Load the device with various types of file archives, (via e-mail and device synchronization protocols) acquire the contents of the device, find and display selected filenames and file contents. • Expect that text, images, and other information contained in the compressed archive formatted files can be found and reported

A distinct set of scenarios was developed for SIM forensic tools. The SIM scenarios differ from the phone scenarios in several ways. SIMs are highly standardized devices whose interface, behavior, and content are relatively uniform. All of the SIM tools broadly support any SIM for acquisition via an external reader. Thus, the emphasis in these scenarios is on loading the memory of the SIM with specific kinds of information for recovery, rather than the memory of the handset. Once a scenario is completed using a suitable GSM phone or SIM management program, the SIM can be processed by each of the SIM tools in succession. Table 8 gives an overview of the SIM scenarios, including their purpose, method of execution, and expected results.

Table 8

Scenario	Description
Basic Data	Determine whether the tool can recover subscriber (i.e. IMSI, ICCID, SPN, and LP elementary files), PIM (i.e. ADN elementary file), call (i.e. LND elementary file), and SMS message related information on the SIM, including deleted entries, and whether all of the data is properly decoded and displayed. • Populate the SIM with known PIM, call, and SMS message related information that can be verified after acquisition; then remove the SIM for acquisition and analysis. • Expect that all information residing on the SIM can be successfully acquired and reported.
Location Data	Determine whether the tool can recover location-related information (i.e. LOCI, LOCIGPRS, and FPLMN elementary files), on the SIM, and whether all of the data is properly decoded and displayed. Location information can indicate where the device was last used for a particular service and other networks it might have encountered. • Register location-related data maintained by the network on the SIM by performing voice and data operations at known locations, then remove the SIM for acquisition and analysis. • Expect that all location-related information can be successfully acquired and reported.
EMS Data	Determine whether the tool can recover EMS messages over 160 characters in length and containing non-textual content, and whether all of the data is properly decoded and displayed for both active and deleted messages. EMS messages can convey pictures and sounds, as well as formatted text, as a series of concatenated SMS messages. • Populate the SIM with known EMS content that can be verified after acquisition; then remove the SIM for acquisition and analysis. • Expect that EMS messages can be successfully acquired and reported.

Foreign Language Data	Determine whether the tool can recover SMS messages and PIM data from the SIM that are in a foreign language, and whether all of the data is properly decoded and displayed. • Populate the SIM with known SMS and PIM content that can be verified after acquisition; then remove the SIM for acquisition and analysis. • Expect that EMS and foreign language data can be successfully acquired and reported.

Synopsis of PDA Seizure

PDA Seizure version 3.0.3.89 is able to acquire information from Pocket PC, Palm OS or BlackBerry devices, including those with cellular capabilities. However, it is not specifically oriented toward cellular phones and omits certain features such as SIM acquisition and examination for GSM phones. PDA Seizure allows the examiner to connect a device via a USB or a Serial connection. Examiners must have the correct cables and cradles to ensure connectivity, compatible synchronization software, and a backup battery source available. Synchronization software (e.g. Microsoft ActiveSync, Palm HotSync, BlackBerry desktop manager software) allows examiners to create a guest partnership between the forensic workstation and the device being investigated.

Pocket PC Phones

The acquisition of a Pocket PC Mobile phone device is done through PDA Seizure with the aid of Microsoft's ActiveSync communication protocol. During the ActiveSync connection an examiner creates a connection as a "Guest" to the device. The "Guest" account is essential for disallowing any synchronization between the PC and the device before acquisition. Before the acquisition of information begins, PDA Seizure places a small dll program file on the device in the first available block of memory, which is then removed at the end of acquisition. Paraben indicated that PDA Seizure uses the dll to access unallocated regions of memory on the device.

To get the remaining information, PDA Seizure utilizes Remote API (RAPI), which provides a set of functions for desktop applications to communicate with and access information on Windows CE platforms. These functions are accessible once a Windows CE device is connected through ActiveSync. RAPI functions are available for the following:

- Device system information – includes version, memory (total, used, and available), and power status retrieval
- File and directory management – allows retrieval of path information, find specific files, permissions, time of creation, etc.
- Property database access – allows information to be gleaned from database information present on the device
- Registry manipulation – allows the registry to be queried (i.e. keys and associated value)

If the device is password protected, the correct password must be supplied before the acquisition stage begins, as illustrated below in Fig. 1. If the correct password is not known or provided, connectivity cannot be established and the contents of the device cannot be acquired.

Fig. 1: Password Prompt (Pocket PC)

During the beginning stages of acquisition, the examiner is prompted with four choices of data to acquire as illustrated below.

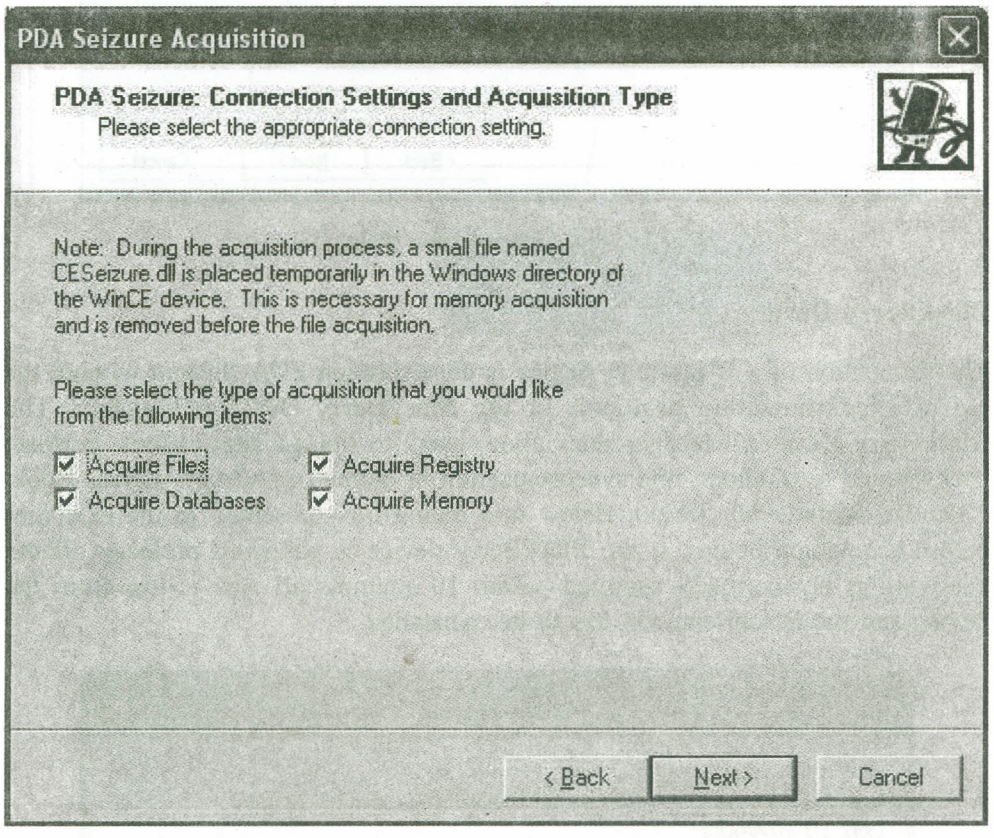


Fig. 2: Acquisition Selection (Pocket PC)

Palm OS Phones

The acquisition of a Palm OS device with cell phone capabilities entails the forensic examiner exiting all active HotSync applications and placing the device in console mode. Console mode is used for physical acquisition of the device. To put the Palm OS device in console mode, the examiner must go to the search window (press the magnifying glass by the Graffiti writing area), enter via the Graffiti interface the following symbols: lower-case cursive L, followed by two dots (results in a period), followed by writing a "2" in the number area. For acquiring data from a palmOne Treo 600, the technique used is slightly different. Instead of

entering console mode via the Graffiti writing area, the shortcut used must be entered via the QWERTY keyboard. Console mode is device specific and the correct sequence of graffiti characters can be found at the manufacturer's Web site. If the device is password protected, the proper password must be entered before acquisition. During the beginning stages of acquisition the examiner is prompted with four choices of data to acquire as illustrated below.

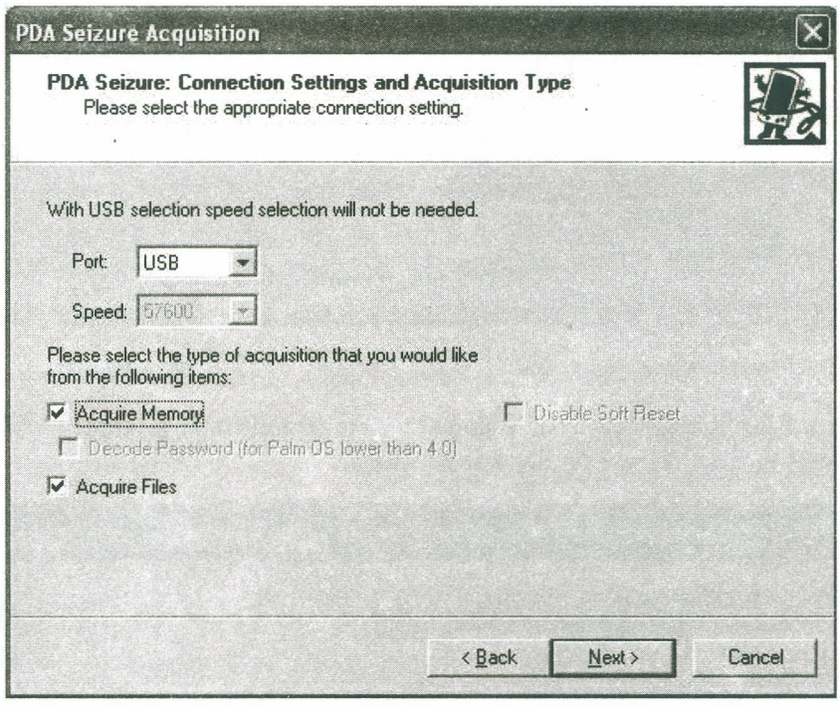


Fig. 3: Acquisition Selection (Palm OS)

BlackBerry Devices

The acquisition of a BlackBerry device is done through PDA Seizure without the aid of synchronization protocols or the BlackBerry Desktop Manager. The BlackBerry Desktop Manager does allow users to upload applications, perform backups and restorations, and synchronization of defined data (e.g. Address Book, Calendar, Memo Pad, Tasks). Below is a dialog box presented to the examiner before acquisition begins, if the BlackBerry device is password protected. If the password is not correctly supplied within 10 attempts all data is lost from the device and the BlackBerry OS has to be reinstalled.

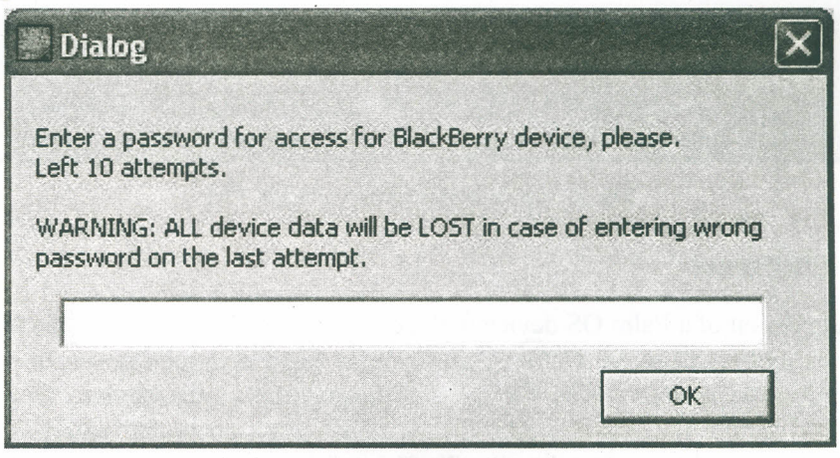


Fig. 4: Password Prompt (Blackberry)

After device selection the examiner is prompted with the following options of acquiring either individual databases, memory, or both.

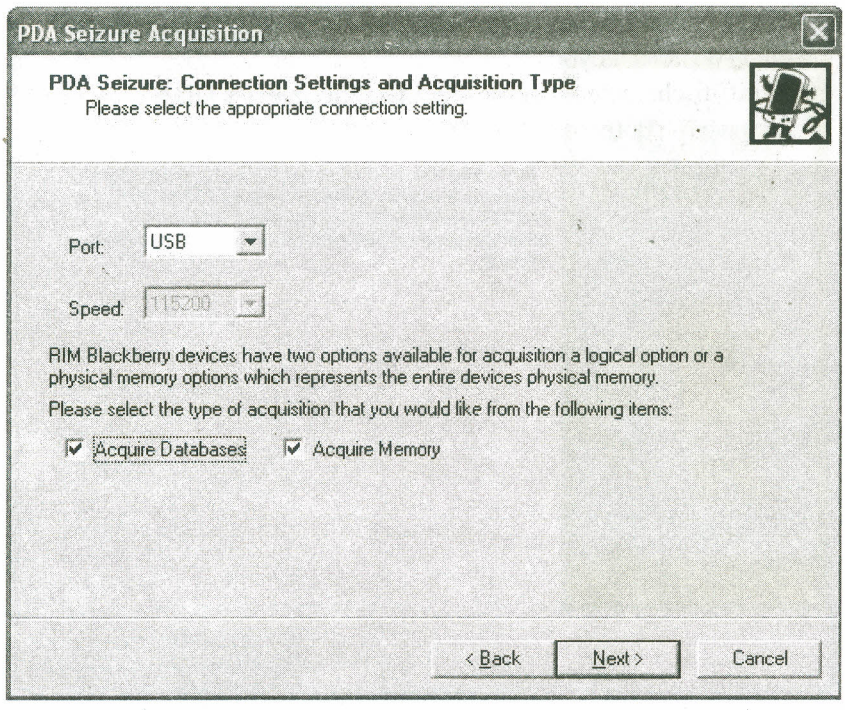


Fig. 5: Acquisition Selection (BlackBerry)

If Acquire Databases and Memory are both selected, the memory is acquired first and then the examiner is alerted that a soft reset will be performed as illustrated below before individual databases are acquired. The soft reset does not affect the device integrity or the integrity of the data associated with the acquisition.

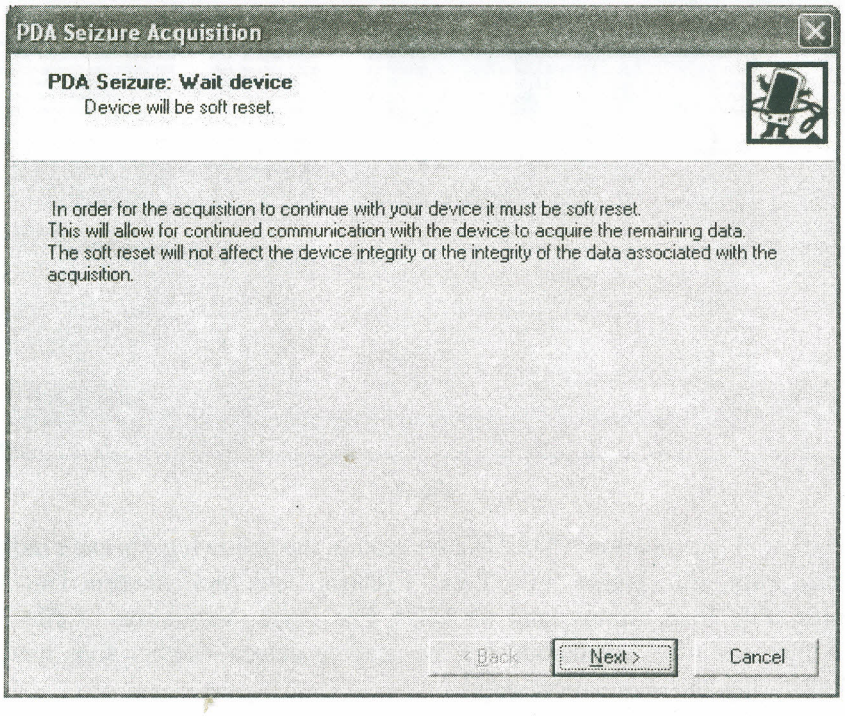


Fig. 6

Acquisition Stage

Two methods exist to begin the acquisition of data from the PDA device. The acquisition can be enacted through the toolbar using the Acquire icon or through the Tools menu and selecting Acquire Image. Either option starts the acquisition process. With the acquisition process, both files and memory images can be acquired. By default, the tool marks both types of data to be acquired. Once the acquisition process is selected, the acquisition wizard illustrated below in Fig. 10 guides the examiner through the process.

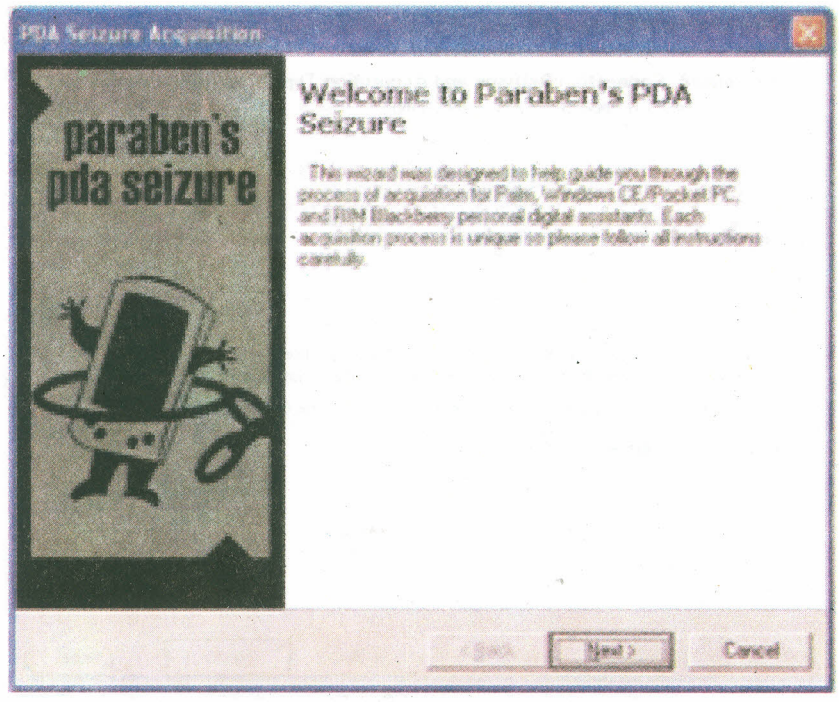


Fig. 7: Acquisition Wizard

Fig. 8 below contains an example screen shot of PDA Seizure during the acquisition of a Pocket PC device, displaying the various fields provided by the interface.

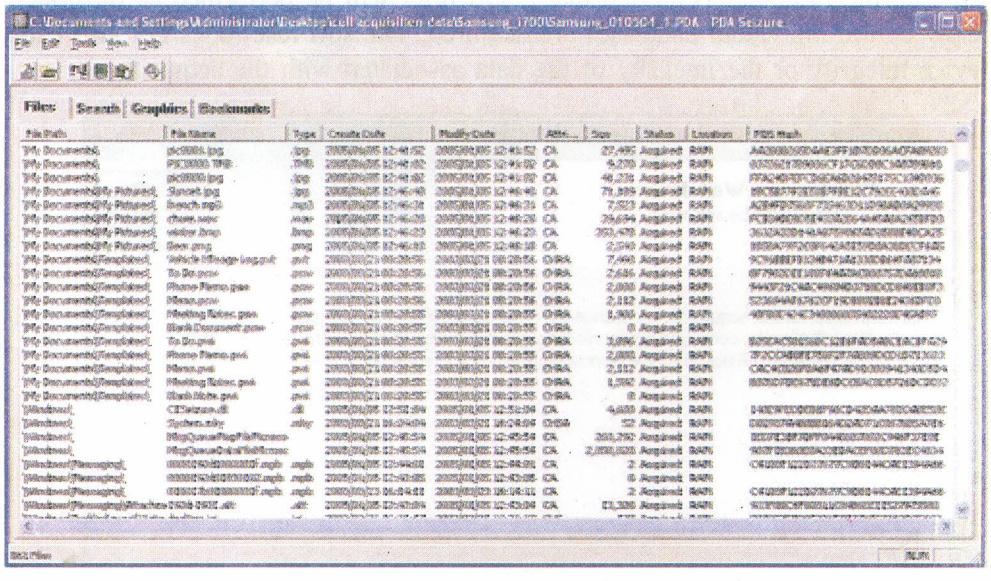


Fig. 8

After Pocket PC acquisition, PDA Seizure reports the following for each individual files: File Path, File Name, File Type, Creation and Modification Dates, File Attributes, File Size, Status, and an MD5 File Hash. Validation of file hashes taken before and after acquisition can be used to detect whether files have been modified during the acquisition stage.

During the acquisition process, CESeizure.dll allows unallocated memory regions to be acquired. The examiner is prompted with check boxes to select one or all of the following before acquiring information on the Pocket PC device: Acquire Files, Acquire Databases, Acquire Registry, and/or Acquire Memory. Each file acquired can be viewed in either text or hex mode, allowing examiners to inspect the contents of all files present. Examiners must use one of the following options to view the files: export the file, launch a Windows application corresponding to the file extension (Run File's Application), or, for Palm OS devices, view the file through the POSE.

Search Functionality

PDA Seizure's search facility allows examiners to query files for content. The search function searches the content of files and reports all instances of a given string found. The screen shot shown below in Fig. 9 illustrates an example of the results produced for the string "homer simpson."

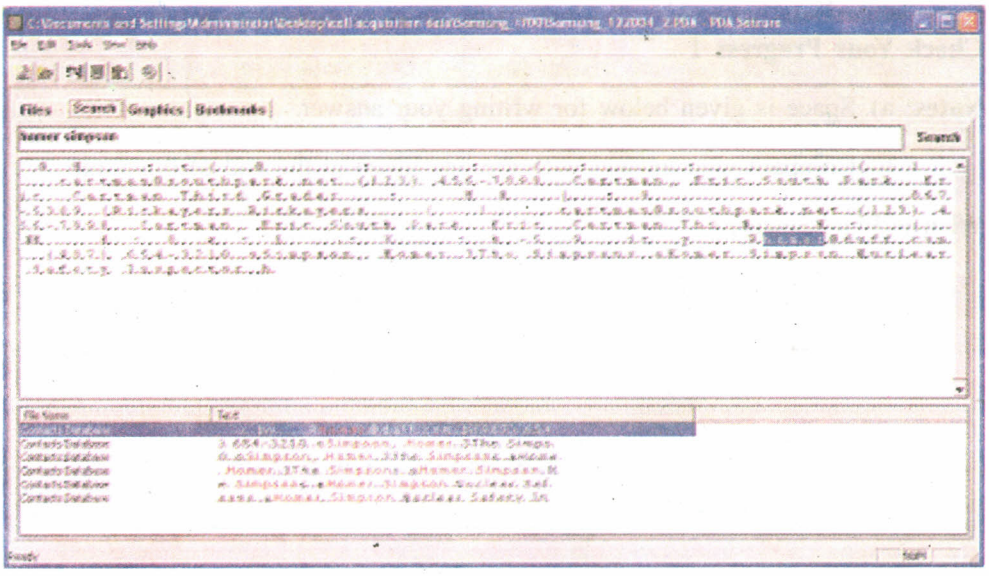


Fig. 9

Report Generation

Reporting is an important task for examiners. PDA Seizure provides a user interface for report generation that allows examiners to enter and organize case-specific information. Each case contains an identification number and other information specific to the investigation for reporting purposes, as illustrated in Fig. 10 below.

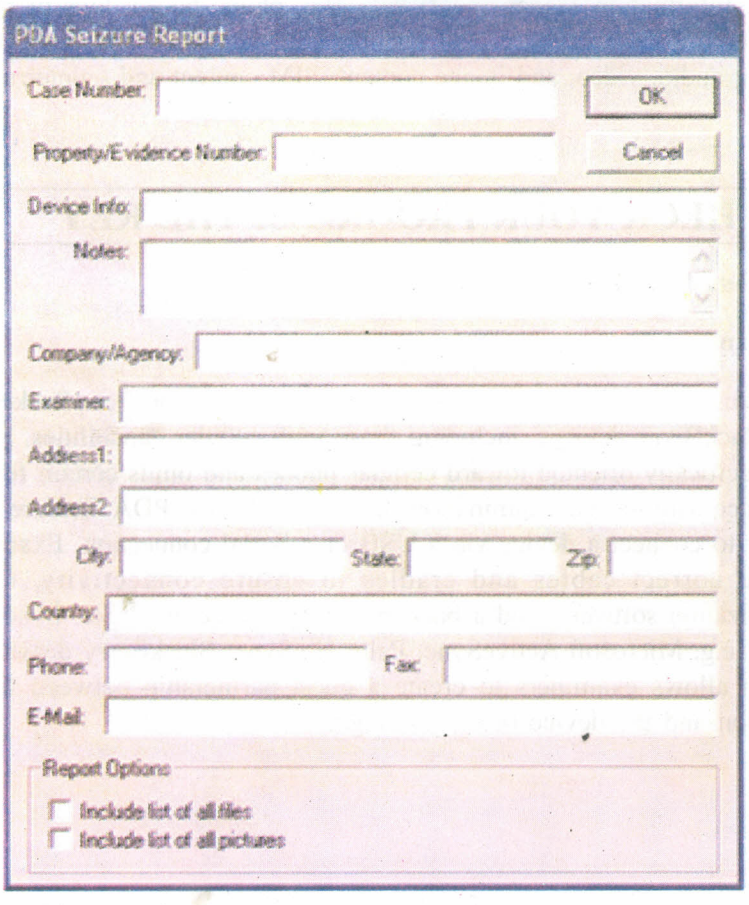


Fig. 10

Once the report has been generated, it produces an .html file for the examiner, including bookmarked files, total files acquired, acquisition time, device information, etc. If files were modified during the acquisition stage, the report identifies them.

Similar procedure can be adopted for all other types of phones and operating systems using different types of forensic tools.

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is PDA Seizure?

.....

.....

.....

.....

.....

4.5 LET US SUM UP

This unit deals with the "forensic examination of mobile devices". While most toolkits support a full range of acquisition, examination, and reporting functions, some tools focus on a subset. Similarly, different tools may be capable of using different interfaces (e.g. IrDA, Bluetooth, or serial cable) to acquire device contents. The types of information that tool can acquire can range widely and include PIM (Personal Information Management) data (e.g. phone book); logs of phone calls; SMS/EMS/MMS messages, e-mail and IM content; URLs and content of visited Web sites; audio, video, and image content; SIM content and uninterrupted image data.

4.6 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

PDA Seizure

PDA Seizure version 3.0.3.89 is able to acquire information from Pocket PC, Palm OS or BlackBerry devices, including those with cellular capabilities. However, it is not specifically oriented toward cellular phones and omits certain features such as SIM acquisition and examination for GSM phones. PDA Seizure allows the examiner to connect a device via a USB or a Serial connection. Examiners must have the correct cables and cradles to ensure connectivity, compatible synchronization software, and a backup battery source available. Synchronization software (e.g. Microsoft ActiveSync, Palm HotSync, BlackBerry desktop manager software) allows examiners to create a guest partnership between the forensic workstation and the device being investigated.

MPDD-IGNOU/P.O.1T/Feb,2012

ISBN-978-81-266-5924-1