An Agent Based Tool for Windows Mobile Forensics

S. Satheesh Kumar, Bibin Thomas, and K.L. Thomas

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

Abstract. Mobile devices are very common in everyone's day-to- day life. Nowadays such devices come with many features of desktop or laptop. Hence people can use these devices for diverse applications. As the acceptability and usability of such devices are very high, there are chances that these devices can be used for illegal activities. The percentage of mobile phones or smart phones involved in cyber crimes is in hike. So it becomes necessary to digitally analyze such devices requiring cyber forensics tools. This paper discusses different types of digital evidence present in Microsoft's Windows Mobile smart phones and an agent based approach for logically acquiring such devices. Also it describes a tool developed for forensically acquiring and analyzing Windows Mobile devices and WinCE PDAs.

Keywords: Windows Mobiles, WinCE, Smart Phones, Cell Phone Forensics, MD5 Hashing.

1 Introduction

The worldwide mobile phone and smart phone sales to end users totalled 1.6 billion units in 2010, a 31.8 percent increase from 2009, according to Gartner, Inc. Also the market for Operating System (OS) based smart phones is in hype than any other devices. Table 1 shows the world wide smart phones sales in 2010 (Gartner, February 2011). The major smart phone sold out during the year 2010 is based on Symbian OS and the Windows Mobile (WM) is in the 5th position. The use of smart phone device has reached in such a situation that it will overtake PCs as the most common Internet access device in the world. Modern smart phones satisfy the functions and features of a laptop or notebook computer. Since these smart phone devices are very common in today's society, they become one way or another involved in criminal activities.

Digital evidence has become one of the major types of evidence in court of laws. In this connection computers and other digital devices have to play key roles in proving cases in litigation process. Since such devices are different from the conventional material objects, specialized tools are required for proper investigation and forensics analysis. There are a number of commercial as well as open source tools for the

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 77–88, 2012.

acquisition and analysis of digital evidence. But most of the tools are used for analysis of storage devices such as hard disks, CDs, Pen Drives etc. Digital forensics science includes a branch called Small Scale Digital Device Forensics, which covers the forensics analysis of Cell phones, Smart phones, PDAs, Gaming/ Audio / Video devices and embedded chip devices. In this area, availability of tools and techniques are limited.

Cell phones as well as smart phones use proprietary OSs. Also these devices use flash memory for data storage. Such OSs and storage media are different from the ones used in desktops or laptops. So the procedures involved in acquisition and analysis of smart phones and other small-scale devices are different. The forensics tools used in acquisition of hard disks or CDs cannot be used in the case of cell phones or smart phones. The file system analysis of flash memory is more difficult as the proprietary OS details are not known. Smart phones need to be switched on before undergoing acquisition, which is not required in the classical computer forensics. Also an acquisition tool developed for a proprietary OS does not work for another OS. Hence it is inevitable that each OS type needs to be addressed separately in cell phone and smart phone forensics.

In this paper we discuss the forensics analysis of Windows CE (Win CE) based Smart phones and PDAs. Here we propose an agent-based approach for the forensics acquisition of WMs and WinCE PDAs. Based on which, we have developed a tool for acquisition and analysis of such devices. Features of the tool and a comparison with some of the existing tools in the market are also discussed. Rest of this paper starts with an overview of the WM OS and is followed by description of the approach proposed. At the end it describes the comparison study.

Table 1. Worldwide Smart phone sales by OS in 2010 (Thousands of Units)

Operating System	Units	Share
Symbian	111576.7	37.6
Android	67224.5	22.7
Research In -Motion	47451.6	16.0
iOS	46598.3	15.7
Windows Mobiles	12378.2	4.2
Other OS	11417.4	3.8
Total	296646.6	100.0

2 Microsoft's Windows Mobile OS

Windows mobile is an advanced mobile device OS based on WinCE kernel. WinCE was introduced with the purpose of providing a compact Windows OS for embedded and compact devices. The OS is divided into 220 modules (exe/dll) and modules are divided into many components. Major feature of WinCE is componentization. A component is a LIB file. It also uses a subset of Microsoft APIs for implementation. The architecture of WinCE devices mainly consists of four layers namely Application, OS, Original Equipment Manufacturer (OEM) and Hardware. Figure 1 below shows the architectural details. Here services are organized into modules, which can be included or excluded when building an image for a specific target system.

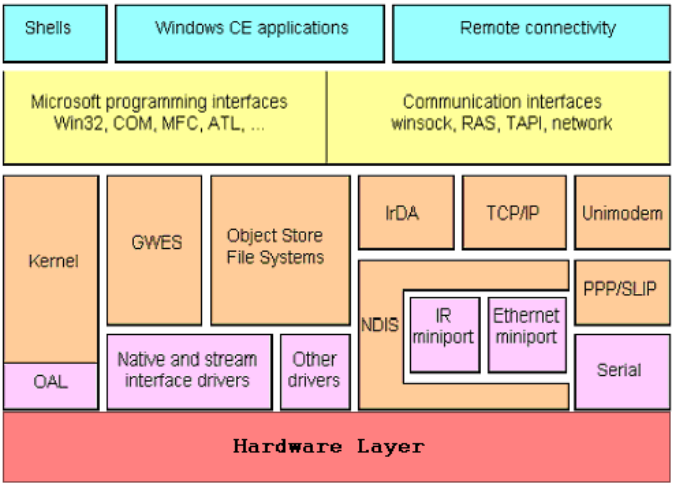

Fig. 1. WinCE Architecture

2.1 Application Layer

Application layer is the interface between the user and the WinCE device. It consists of programming interface, embedded shell, communication interfaces, win 32 APIs such as Winsock, RAS, TAPI, etc. It also includes the connectivity services with the external devices.

2.2 Operating System Layer

Operating System Layer includes kernel and device drivers, which are used to manage and interface with hardware devices. Device drivers provide the linkage for kernel to recognize the device and to allow communications between hardware and applications. The Graphics Windowing and Events Subsystem (GWES), which is part of OS, provides the interface between user, application, and OS. GWES is an integrated graphics device interface (GDI), window manager and event manager. The object

store refers to the file system used in the device. It is sub divided into three types of persistent storage - File system, Registry, and WinCE databases.

The file system supports a file to be stored both in RAM and ROM. User can access some of the ROM files. Information like Contacts, SMS, Call logs etc are not stored as files in WinCE devices. These are stored as databases, which are repository of information. The Windows CE registry is a database that stores information about applications, drivers, system configuration, user preferences, etc. Registry is the area for storing the settings of OS, applications, and user. Registry is volatile as it is always stored in RAM. Windows CE can regenerate a default registry from a file stored in ROM, when no registry is available in RAM.

2.3 Original Equipment Manufacturer Layer

The OEM Layer is the one between Operating System and Hardware layers. It includes OEM Adaptation Layer (OAL), which consists of a set of functions related to system start-up, interrupt handling, power management, boot time hardware detection, profiling etc. Once written, OAL is statically linked to kernel. The OAL also allows an OEM to adapt WinCE to a specific platform.

2.4 Hardware Layer

Hardware layer represents bare hardware part of the device. WinCE supports wide range of processors including ARM/StrongARM, MIPS, PPC, SuperH, and X86. It also supports MIPS16 and ARM Thumb Processors. The hardware layer also includes flash memory, communication interfaces, memory controller and power manager.

3 Cyber Forensic Process

When mobile devices are included in a crime, it becomes necessary to identify, acquire and analyze such devices to bring the culprit before a court of law. Cyber crime investigation involves many processes, which are not usually followed during a conventional crime investigation. The important processes involved in a cyber crime investigation are evidence identification, seizure, acquisition, authentication, analysis, presentation and preservation. Each step is so important that at any point of time during the case trial, court can direct the investigation agency to repeat any step or can assign a third party to repeat the entire forensics process. In order to perform the forensics analysis accurate and perfect, cyber forensics tools play a major role. The processes, which require forensics tools, are acquisition, authentication and analysis. Here in windows mobile analysis also, we need tools for the forensics processes.

3.1 Identification

Identification of digital evidence is the key process in cyber forensics. The evidence produced before a court of law should be admissible, authentic, reliable and believable. Unless first responders search and identify all available evidence from the scene of crime, the case cannot be proved at the court. Hence evidence identification ultimately determines the success of a case at the court.

3.2 Seizure

Seizure is the process of physically collecting identified evidence from the scene of crime. During seizure process, all digital equipments need to be collected. Also it is advised that a hash value of all storage devices needs to be generated at the scene of crime itself. This is to avoid suspect's claim that evidence is manipulated or tampered by investigation agency or first responders.

3.3 Acquisition

In computer forensics, priority and emphasis are on evidential integrity and accuracy. Doing analysis directly on original evidence might change or alter the evidence. So, it is essential to have a forensically sound copy of the original evidence for analysis. The process of generating an exact replica of the suspect storage media or memory is called acquisition. The acquisition process is carried out at the forensics lab, as it requires a sterile destination storage device for storing the acquired image.

3.4 Authentication

Digital evidence can be easily altered at any point of time after the seizure. Once the police or any other investigation agency seizes evidence, its content should not be changed. In order to assure the evidence's integrity, authentication process is introduced. Taking hash value of the storage media carries out authentication. During acquisition, hash values of original evidence and acquired evidence are generated. If both the hash values are same it shows that the image acquired is an exact copy of the original evidence. This is how credibility of acquired image is proved in the court of law. Also during the trial, court can ask to perform a new hashing process, when the credibility of the evidence is questioned. The standard algorithms used for hashing are MD5, SHA1, and SHA2.

3.5 Analysis

This is the major step in cyber forensics process where acquired image is analyzed for identifying actual evidence, which can prove the involvement or non-involvement of a suspect in the case. A forensic analysis can reveal much information like websites visited, files down loaded, files last accessed, files deleted or modified, renamed files,

files whose extension is changed, encrypted files etc. A thorough analysis takes much time depending upon the size of the image analyzed, nature of the case reported etc.

3.6 Presentation

Once analysis is completed and the analyst comes out with a conclusion, a case analysis report need to be prepared for presentation before the court. The report should have a standard format, should be authentic (can also include a hash values of the report data) and should submit both hardcopy and softcopy. The report should contain attached documents in support of the inference proposed. The report should also include details about the tools used, its version, expert's bio-data and qualification etc.

3.7 Preservation

Trial of a case normally takes years to complete. And it is mandatory that evidence needs to be preserved till end of the final judgment. Since digital evidence is highly volatile and fragile, it needs to be preserved in a cool, dry and secure place. It should also be kept away from generators, magnets etc. Also a proper chain of custody of evidence should be maintained since this can be challenged at the court at any point of time.

4 The proposed Approach

The forensics process of WM smart phones consists of basically two steps - acquisition and analysis that require separate software modules. The acquisition module is intended to (logically) copy file system present in the device. The best forensics practice is to physically image the suspect media, i.e. the Bit Stream Imaging. But since windows mobiles use NAND/NOR flash memory and which is divided into ROM and RAM, the entire memory cannot be acquired physically [11]. Unless we have a full physical image and a file system, the data cannot be properly decoded or analyzed. Hence usually logical copy of the object store is carried out in such devices. During acquisition, the tool should support to access the entire object store content (file system, databases and registry) and copy to a destination storage medium like a hard disk or pen drive. The proposed agent based approach is discussed below.

4.1 Requirements

The device, which is to be acquired, should be connected to a desktop PC either through Bluetooth or USB cable. This is for establishing a channel for to and fro data transfer between mobile device and PC. In order to synchronize mobile device with desktop PC, Active Sync or Windows Mobile Device Centre (WMDC) software, which is freely available in the Internet, need to be installed on the PC. When the device is connected to desktop PC, the software will automatically detect mobile device and a connection will be established.

4.2 Forensic Data in the Device

As explained in the section 2.2, object store in the device is divided into file system, database and registry. Data stored in the device consists of file and folders, phone information, SMS, Call logs, Emails, Address book, Tasks, To-Do list, Calendar, Photos, etc. In addition to these, registry is stored in RAM. These are forensically important data, which need to be acquired for analysis.

4.3 Agent Based Acquisition

The tool developed for acquisition is based on a client server approach. The client part is installed on desktop PC and server agent is copied onto mobile device before acquisition starts. The agent, which is a .cab file, needs to be installed on the mobile device for accessing databases. The client initiates acquisition process and the server agent reads data from mobile device and sends to the client application listening at the desktop side. The client application receives data and stores in the desktop PC as an image file. The client application is provided with a graphical user interface (GUI) window where user can select different options such as SMS, Call logs, Contacts, Emails, Calendar, Tasks, Phone information, registry, files/folders, etc for acquisition. Depending upon the option selected, the client program will either access and copy logical files and databases using Remote APIs or initiate an agent present in the mobile device to access, read and send the data to the client application using Messaging APIs or Phone APIs. The agent application is removed from mobile device after completing acquisition process. Agent was implemented in such a way that it would not change or alter any databases present in the mobile device. During acquisition process, client module also generates hash values of the acquired files and databases, which will prove the authenticity of acquired evidence.

4.3.1 File System and Registry Acquisition

The data stored in the mobile device are in different formats. The file system and registry in the object store can be accessed from desktop PC using Remote Application Programming Interfaces (RAPI). The tool includes a client module, which supports acquisition of file system, registry and some of the databases using RAPI from mobile device.

4.3.2 Database Acquisition

The Remote APIs do not support acquisition of the database files *pim.vol, cemail.vol* and *clog.db* from mobile device. These files are very important as they store details like Contacts, Tasks, Appointments, SMS, Emails, Call logs, etc. In such a situation Messaging APIs and Phone APIs are to be used to access such information from the device. In order to access databases from mobile device, an agent is uploaded to the mobile device before acquisition. If user selects any database contents at the client side for acquisition, the corresponding API function will be initiated in the server agent. After that, agent will read data from mobile device and will send databases to the client. Since the agent accesses restricted databases, which require permissions, a

code signed agent need to be installed for database acquisition. In this tool, a code signed agent is used for database acquisition. The file system, registry data and e few database acquisition, which are acquired using the RAPI calls, do not require such a digital signature as the agent is not used in that case. After completing acquisition process, image is stored in the desktop PC, which can be further loaded on the analyzer module for analysis.

5 Acquisition and Analysis Tool

The tool developed for forensic acquisition and analysis of windows mobiles has two modules; one is for acquiring the device and the other is for analyzing acquired image. The analysis module is intended for analyzing acquired image content and displaying files and folders, registry and databases in separate file viewers.

5.1 Features of the Acquisition Module

The acquisition module is developed as a standard digital imaging tool. This has a GUI, which will collect the case related information before starting acquisition process. The investigator can add case details such as place of seizure, police station, nature of crime, suspect name, etc at the time of acquisition. He can also include investigator name, rank, seizure number, etc. It also provides an option for selecting file system, registry and databases such as SMS, Call logs, Contacts, etc for acquisition. The tool also supports to generate MD5 hash value of the acquired image. Figure 2 and 3 shows the various steps involved during acquisition process.

After acquisition, the tool will generate two files. One is the acquired image file, which is *a .pmg* (a format that we defined) file and the other is an html report file. The html report file includes case details entered by the investigator, device details and the names of all file and databases along with individual hash values. Since media hash value of mobile phone is different when performing back-to-back acquisition [10], it is advised to take individual file hashes to prove the authenticity of cell phone evidence.

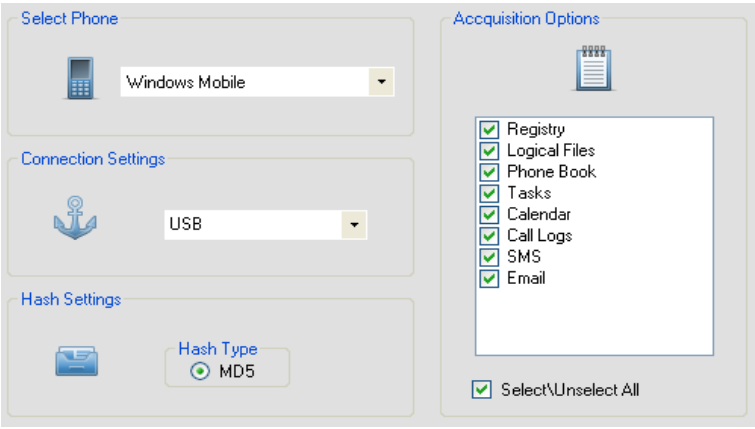

Fig. 2. Device acquisition settings window

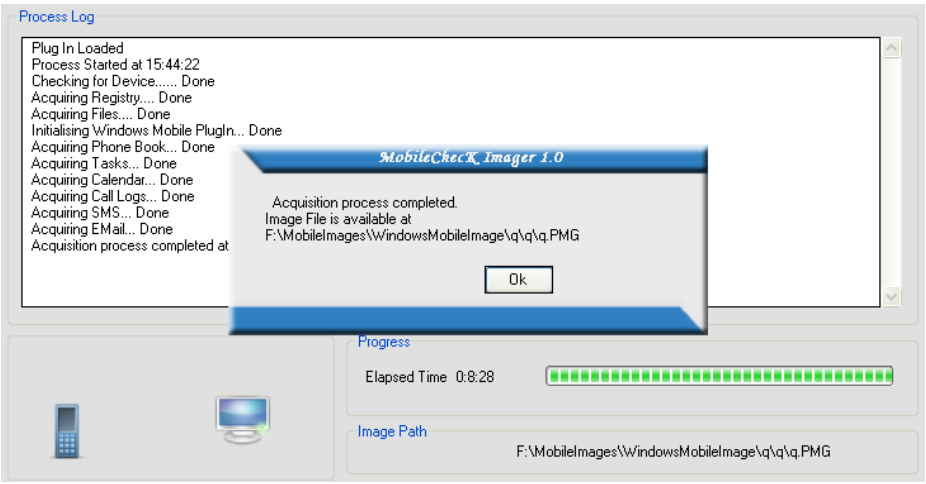

Fig. 3. Window showing device acquisition completion

5.2 Features of the Analysis Module

The analysis module is used to display and decode the image created during acquisition. The tool includes all features of a standard forensics analyzer. It supports Text, Hex, Picture and Gallery Views. When an image file is loaded in the tool, it will show all the folders and databases in the left pane as a tree view. The databases include the Phone Information, Phone book, Tasks, Calendar, Call logs, Emails, SMS etc. When any one of the tree view item is selected, its content will be displayed in the right pane. Figure 4 shows Phone information displayed in the right pane.

The most important forensic information available in mobile phones and smart phones are Contacts, Call logs and SMS. This information will help investigation agencies to get some cues for further investigation. Our tool shows all these information in separate file viewers. Incoming, outgoing and missed call details are displayed separately. Also Inbox, Outbox, Draft, Sent and Deleted SMS are categorized in separate viewers. The analysis tool is also provided with keyword and file search facilities, which are the key features of a forensics analysis tool. User can add any keyword or file extension in the box provided and the tool will search entire image for the string entered. It shows search hits in a separate viewer. The tool has book marking facility, time line display of files and folders, summary view of files, hash verification facility, file exporting, etc. The timeline facility helps to identify files based on created, modified or accessed time. This will ease a user to confine his analysis to files created/modified/accessed over a particular period of time.

The tool also generates an analysis report. The report file contains device details, names of files and databases along with the hash values. It also supports to append evidence files to the report wherever it is necessary. The tool has another feature called multiple evidence analysis. User can load more than one evidence image file at a time and perform analysis simultaneously. Figure 5 below shows contents of a phone book.

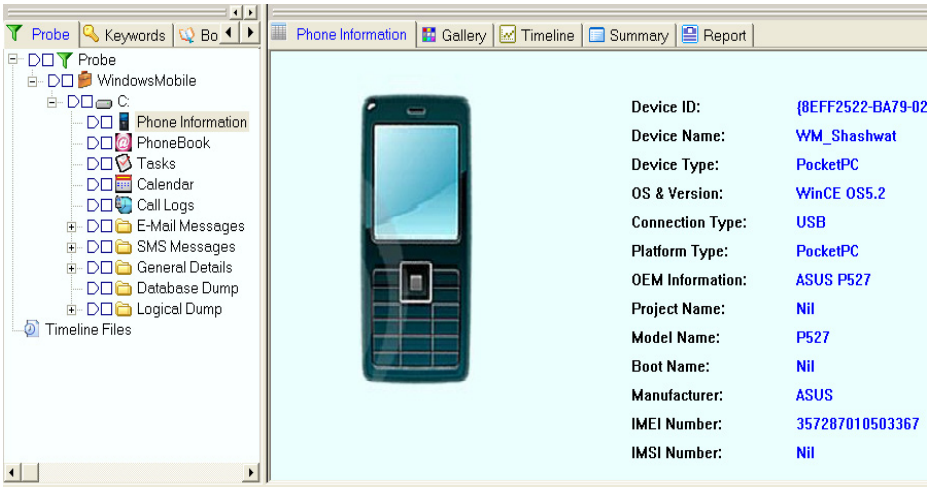

Fig. 4. Phone Information

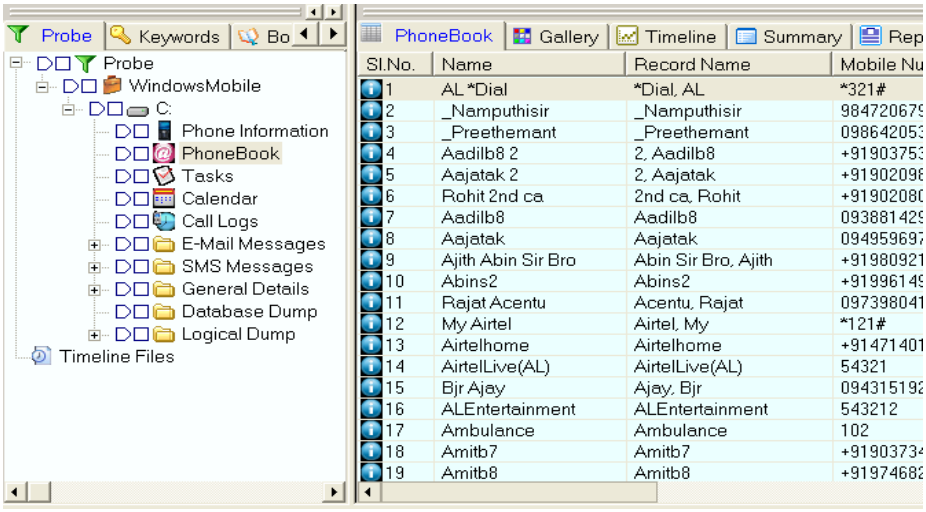

Fig. 5. Phone Book display

6 Tool Comparison

There are number of software as well as hardware tools in the market for forensics analysis of WM smart phones and WinCE PDAs such as Paraben's Device seizure, Oxygen Forensics tool, CelleBrite's UFED, etc. The following table 2 gives a comparison study of the proposed tool with major commercial tools available in the market. Here comparison is conducted only for WM smart phones; it is not carried out for any other phones. The study has been carried out using the Paraben's device seizure version 3.3, Oxygen's forensics tool version 1.2 and UFED with software version 1.5.5.6.

Table 2. Comparison of our tool with other commercial tools

Features / Tools	Contacts	SMS	Call Logs	Tasks	Calendar	Device Info	Memory Details	File System	Registry
Paraben's Device Seizure	✓	✓	✓	✓	✓	✗	✗	✓	✓
Oxygen 's Forensics Tool	✓	✓	✓	✗	✓	✓ *	✗	✓	✓
Celle-Brite's UFED	✓	✓	✓	✗	✓	✗	✗	✓	✗
Proposed Tool	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Only partial information

The major features of our tool are that it provides device information, owner information and memory details, which are not provided by any of the other tools. The device information includes IMEI number, device ID, OS type and version, Model name, Owner information, Manufacturer, Platform type, OEM information, etc. Since there are number of phones in the market, this device information is very important as it proves identity of a particular device. Memory details include size of memory used, actual Physical memory, available Physical memory, Actual virtual memory and available virtual memory. Our tool also supports acquisition of E-mails, which is not there in the above tools. The tool acquires and displays Inbox, Draft, Outbox, Sent and Deleted mails from the device. Like any other tool, which uses an agent for database acquisition, our tool also removes the agent from mobile device after completing acquisition process. This approach helps to perform a complete acquisition of databases, files and registry of WM devices. Our tool is a total forensics solution for WM smart phones and WinCE PDAs.

7 Conclusion

In this paper, we discussed a method to acquire windows mobile devices using client server approach. The file system and registry data are acquired without using an agent. But in order to acquire important databases such as Contacts, SMS, Call logs, E-mails, etc an agent is uploaded on to the mobile device. Also agent-based approach requires Messaging APIs and Phone APIs for implementation. The agent cannot be run on the target mobile device unless it is signed by Windows Mobile's code signing authority. This is because the agent requires a code signing in order to execute within the mobile device. We have used a signed agent for database acquisition. Our tool

will work in all WM OS versions up to 6.5. The tool is tested with ASUS P 527, Sony Ericsson XPERIA X2 and Hp iPAQ Pocket PC. In all of the above devices the tool worked without fail.

References

1. Jansen, W., Ayers, R.: Guidelines on cell phone forensics, National Institute of Standards and Technology, Special Publication 800-101 (2007)
2. Ayers, R., Jansen, W., Cilleros, N., Daniellou, R.: Cell phone forensic tools: An overview and analysis. Technical Report NISTIR 7250, National Institute of Standards and Technology (2005)
3. Carrier, B.: Defining Digital Forensic Examination and Analysis Tools, Digital Forensics Research Workshop II (August 2002)
4. Mellars, B.: Forensic Examination of Mobile Phones. Digital Investigation. The International Journal of Digital Forensics & Incident Response 1(4), 266–272 (2004)
5. Ayers, R., Dankar, A., Mislan, R.: Hashing Techniques for Mobile Device Forensics. Small Scale Digital Device Forensics Journal, 1–6 (2009)
6. van der Knijff, R.: Embedded Systems Analysis. In: Casey, E. (ed.) Handbook of Computer Crime Investigation, ch. 11. Academic Press (2002)
7. Kruse II, W.G., Heiser, J.G.: Computer Forensics – Incident Response Essentials. Pearson Education (September 26, 2001)
8. Logsdon, B.: Compaq iPAQ Parrot Talks: How to flash your ROM by the backdoor. Pocket PC Passion (February 2001)
9. Architectural Overview of Windows Mobile, Windows Mobile 5.0 and 6-powered Devices, White Paper, Published by Microsoft (May 2007)
10. Danker, S., Ayers, R., Mislan, R.P.: Hashing Techniques for Mobile Device Forensics. SSD Journal 3(1) (June 2009)
11. Fiorillo, S.: Theory and practice of flash memory mobile forensics. In: Proceedings of the 7th Australian Digital Forensics Conference (December 2009)