Digital Evidences of mobile devices and investigation (MOBILE FORENSICS)

[1] Smit.S.Patel, [2] Priyanka Sharma
[1] Student M.Tech(Cyber Security), [2] Professor (IT)
[1,2]Department of Information Technology
[1,2]RakshaShakti University, Gujarat-Ahmedabad, India.

ABSTRACT

The Google's Android mobile platform has quickly risen from its first phone in October 2008 to the most popular mobile operating system in work by early 2011. The explosive growth of the platform has been significant win for consumers with respect to competition and features. However forensic analysis and security engineers have struggled as there is lack of knowledge and supported tools for investigating these devices. This paper presents efficient generalized forensics framework for acquisition and subsequent analysis of these devices.

Keywords: Digital Evidence, Mobile Forensics, Tools, Digital forensic Investigation Process, Smartphone Forensic, Security, Open Architecture, Acquisition methodology, Forensic prospective, Acquisition Algorithm

1. INTRODUCTION

According to Nielsen January 2012 survey, 46.3 percent of all smartphone owners have an Android device. But, 51.7% of recent acquirers of new smartphones have chosen Android devices over Apple iPhone [1].

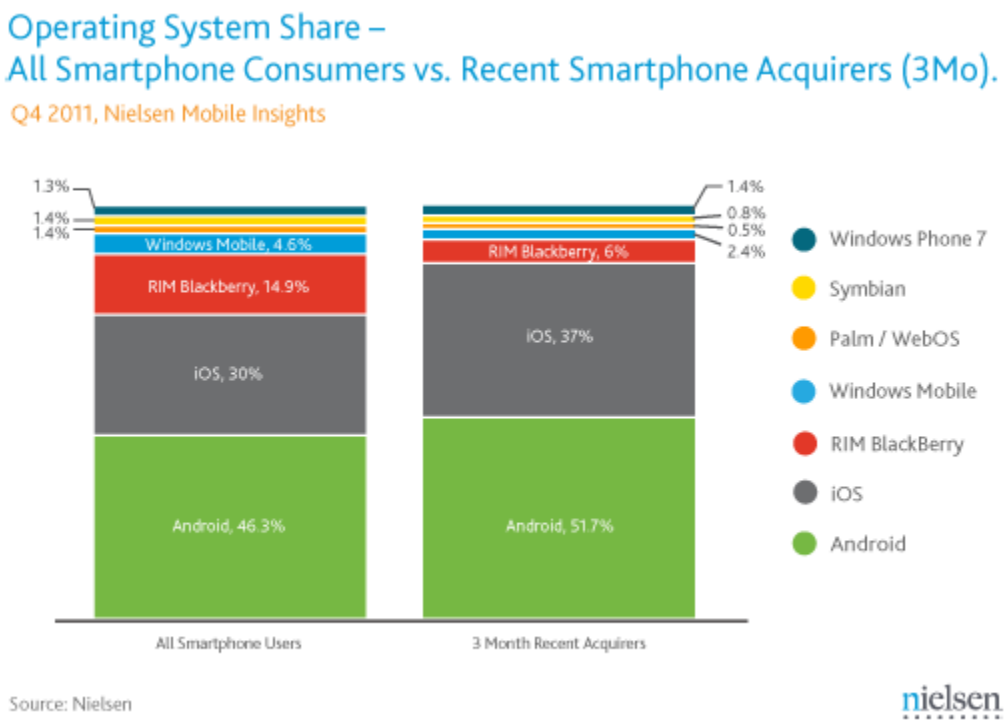


Fig. 1Operating System Share- Nielsen 2011

Although most of the discussed statistics about Android focus on smartphones and now tablets, there are many more devices that currently or in the near future will run on Android. Some examples include vehicles, televisions, GPS, gaming devices, netbooks, and a wide variety of other consumer devices. These smartphone devices are getting more and more sophisticated in terms of processing power and available features making them equitable to modern PC's. But, this is also posing important security risk of these devices being used for carrying out digital crimes or being target of a security attack due to predominant use by employees at various enterprises. IT firm IBM has warned that malware targeting mobile devices is on the rise with the tripling of critical vulnerabilities this year compared to last year. The IBM report cited the G Data Security Labs' findings that the number of smartphone and tablet malware increased 273 percent in the first semester of 2011 compared to the same period last year. As Android devices grow in numbers, an increased awareness of the data they possess will equally grow. Unfortunately, much of that interest will come from cyber-criminal organizations who realized that successful attacks against the platform will yield significant results as the devices contain enormous quantities of personal and business information. Android devices have also been vulnerable to various kinds of security and malware attacks. According to McAfee in their new study, the number of viruses, Trojans, and other rogue pieces of code aimed at Google's Android platform shot up 76 percent. Lots of similar security vulnerability reports keep coming about Android platform almost regularly now. However forensic analysis and security engineers have struggled as there is lack of knowledge and supported tools for investigating these devices. This paper tries to analyze issues not only providing in-depth insights into Android hardware, software and files system but also by studying techniques for the forensic acquisition and subsequent analysis of these devices [10].

RELATED WORK

Currently, numbers of researchers had addressed to the security issues of the smartphone, and developed various technologies for the investigative features. In this section, we have analyzed the definitions of digital evidence, mobile forensics and smartphone, and also introduced some studies that had down in Android smart phone operating system architectures, and mobile phone forensic tools area [2].

A. Digital Evidence

The digital evidence is a series of binary digit numbers on transmission, or stored information files on the electronic device. Moreover, the digital evidence file formats includes audio, video, images, and digital, etc. The digital evidence is not virtual exist, but there are some other features to look for, the digital evidence can be copied with unlimited differences, can be modified easily, hard to be identified the original resource, can be integrated data verification, and cannot be understood directly without technical process [3].

B. Mobile Forensics

With the increased emphasis on social security issue, crime issue is considerable when it comes to the utilization of smart phone technologies, digital forensics provide the technical skills to collect evidences for the court to review and judge cases. Digital equipment has changed daily, people has pervasive use some common digital devices such as computers, Internet, mobile phones, digital cameras, hardware, storage devices, etc. Currently, digital forensics has widely used in the areas of network forensics, mobile forensics, computer forensics, and memory forensics, etc. According to NIST definition of mobile phone forensics process is preservation, acquisition, examination and analysis, and then reporting [5].

C. Smartphone

Due to the advanced technological development, mobile phone's selling was decreased in 2009; smart phones' selling is increased, and the commercial demand cannot be sacrificed by the smart phone. In Table 1 shows definition of smart phone, the various categories of smart phones' forensic, different operating systems and the disordered domestic laws for forensic procedures result in the difficulty of smart phone forensics [5].

BACKGROUND: MOBILE AND ANDROID FORENSICS Google's Android is an open source smart phone operating system, which is based on Linux [4].

A. **History of Android**

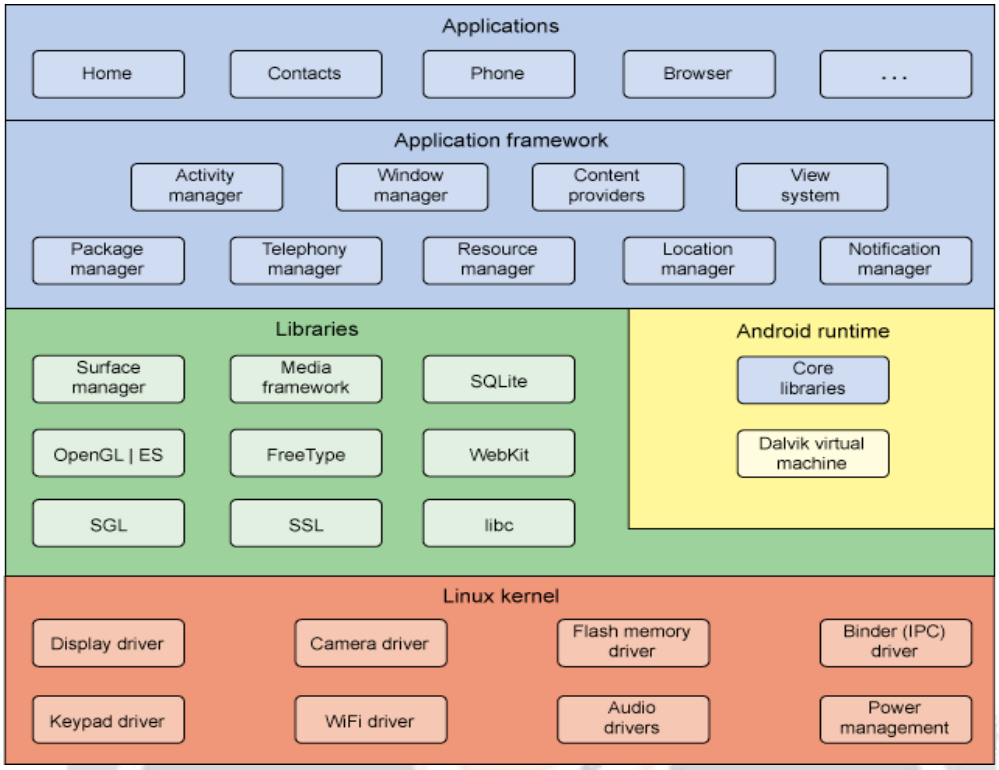
A central figure in the development of Android is Andy Rubin and his company "Android, Inc." formed in 2003 which was subsequently acquired by Google in July 2005. On November 5th2007, Andy Rubin announced Android as an open and comprehensive platform for mobile devices to be further developed by "Open Handset Alliance" comprising of more than 30 technology and mobile leaders including Motorola, Qualcomm, HTC and T-Mobile. In 2007, Google released an early look at the Android software development kit (SDK) to developers followed by first Android Developer Challenge. The top 50 apps are available for review here [3].

B. Android OS

Android's kernel is a fork of the Linux kernel but has further architecture changes by Google outside the typical Linux kernel development cycle. For example Android does not have a native X Window System nor does it support the full set of standard GNU libraries, and this makes it difficult to port existing Linux applications or libraries to Android. The open strategy behind Android naturally let to the release of Android source code through AOSP on October 21, 2008 [10].

C. Android Architecture

Android is composed by five major components, depicted in Figure 2 that are briefly introduced below:



• **Applications:** Android is distributed with a set of typical applications for Mobile devices (e.g., e-mail client, text messaging management, browser, contacts management) written using the Java Programming Language.

• **Application Framework:** Android offers the capability of Java applications development providing a rich set of services which can be exploited. Developers can consume and provide services through of a wide set of Application Programming Interfaces (APIs), with the objective of the reuse of components, always respecting the security constraints enforced by the framework [5].

• **Libraries:** Android includes a set of libraries (e.g., Standard C System Library, Media Libraries, 3D Libraries) used by the components of the system through the Android Application Framework just outlined [6].
• **Android Runtime:** The Runtime is composed by a set of Core Libraries and by the Dalvik Virtual Machine (DVM). Every running application holds its own instance of the DVM and executes in its own process [1].
• **Linux Kernel:** One of the most interesting features of Android is the underlying Linux kernel supporting the core services, such as memory and process management, network stack, drivers and security [1].

D. Overview of Android File System

Another interesting element of Android is the natively supported YAFFS2 File System (FS). YAFFS stands for **Yet Another Flash FS** and, at the time of writing, it is the only FS that has been specifically designed for NAND flash chips. The use of NAND flash chips in the field of embedded and mobile devices is increasing and replacing the common-old NOR chips because of the improved density, speed and the reduced cost. At the time of writing, YAFFS was released in two version: YAFFS1: designed for old NAND chips with 512 byte pages plus 16 byte spare areas; YAFFS2: evolved from YAFFS1 to accommodate newer chips with 2048 byte pages plus 64 bytes spare areas. In addition to the different NAND chips supported, YAFFS2 evolved in terms of performance, reliability, efficiency and support to the "write once" requirement for modern NAND flash [3].

E. Android Security Architecture

Android is a multi-process platform which relies on the standard Linux facilities for processes and users management; in fact, most of the security between applications is enforced at process level exploiting such standard facilities. However, in order to support the reuse of components and the provisioning of services between different applications, some finer-grained security features are provided by the mechanism of permissions [5].

• **Applications and sandboxes:** Android, by default, denies to any application the capability to perform operations with the objective to hamper any other application, the OS or the end-user. Hence, due to this design pillar, for applications it is impossible to perform any operation on end-user private data (e.g., contacts, messages), to gain access to another application's files, to perform network accesses, to manage the device state, and so on. Following this idea, Android binds any running application to a secure Sandbox which cannot interfere with any other applications, except by the explicit declaration of the required permissions to access to the desired capabilities which are not provided by the Sandbox. The set of permissions held by an application is defined in a static way, verified at installation time and cannot change during the lifetime of the application. Any Android application is required to be signed with a certificate, held by the developer, in order to establish and to manage relationships between applications [6].

• **User IDs and permissions:** By default, Android manages each installed application as a different Linux user; in fact, at installation time, any application is provided with its own unique Linux user ID. All the data stored by a given application will receive the application's user ID as well; to grant to other applications any access to such data, it is required to enable the access from the Others group of Users By default, a basic Android application has no associated permissions; in order to overcome the limitations which could arise using only the DVM default capabilities, and to allow service provisioning between applications, it is possible to declare further permissions. The declaration of the needed permissions is performed at development time through the inclusion of <uses- permission> tags in the application's Android manifest.xml file. During the installation, the permissions required by the application are granted by the package installer module; the policy to grant permission can leverage both on applications' signatures and on interaction with the end-user. Once the application is installed, the set of the granted and denied permissions is built and cannot be modified: during the execution, no more checks are performed [10].

F. Android: Important Data From Forensics Perspective

Following data can be considered as important from forensics perspective on Android devices:

- Subscriber & equipment identifiers
- Phonebook
- SMS, Text Messages
- Electronic mail
- Audio and video records
- Instant messages
- Location information [7]
- Date/time of calls, movements, etc
- Appointment Calendar
- Dialed, incoming, & missed call log
- Photos
- Multi-media messages
- Electronic Documents

All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL your paper, you must type out the address or URL fully in Regular font [13].

I. LITRACURE REVIEW

Forensic investigations historically have a basic four-step process when dealing with evidence. The evidence must first be collected or seized to maintain its integrity as evidence. Investigators examine the evidence using the required tools or methods. The results of the examination are then analyzed and the

conclusions are then reported (NIST, 2006). This process combined with chain of custody procedures will help persuade the court that the integrity of the evidence has been maintained (Kruse, 2005).

This process occurs for all items of evidence in any investigation whether the evidence is fingerprints or digital data on a hard drive. Computers store data on non-volatile storage media called hard disk drives. Data on a hard disk drive is stored by placing positive or negative charges that represent ones and zeros to a set of spinning plates or platters. The computer's software interprets these ones and zeros into information 2the individual can use. Data typically remains on the drive, even if the user deletes the data. When new data overwrites the old, the old data is gone (Carrier, 2005). The collection process for digital evidence found on a computer's hard drive may include two basic parts.

First the physical drive may be collected to preserve the original evidence, and second the data (the actual evidence) contained on the drive must be collected for analysis. To collect the physical drive traditionally The United States Secret Service recommends investigators pull the power plug from the computer (United States Secret Service, 2010). This action immediately cuts power to the computer, and thus the hard drive, preventing it from writing or erasing data from the drive. The data is now preserved on the hard drive at the exact moment power was removed. This method, however, can cause issues if the drive is password protected, has encrypted volumes, or had evidence that is now lost when the volatile memory disappears.

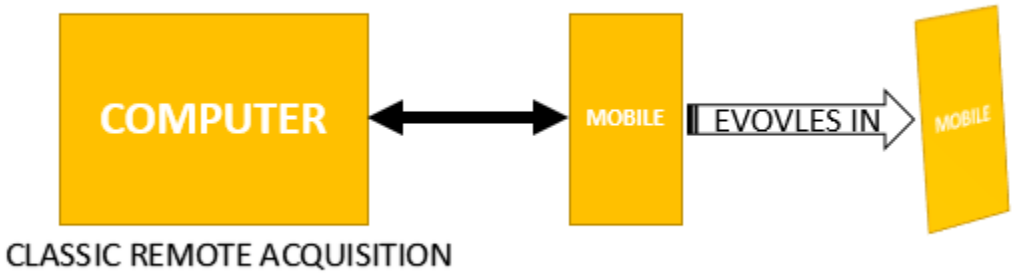
To examine the data the suspect drive is removed from the computer and connected to a write blocker. A write blocker is a device that prevents the examination computer, or the user, from writing or changing data on the suspect drive (Carrier, 2010). Using specialized software, the investigator then creates an image file that is an exact copy of the drive. The investigator can verify that the drive image is an exact copy by comparing the MD5 hash values (NIST, 2006). If the hash value of the suspect drive and the new image match, then the process was successful. This duplicate image allows the investigator to analyze the data without risking damage or modification to the original data.

Hard drives are non-volatile media, which means they maintain the data contained on them even after power is lost to the drive. Computers also use memory to store live or volatile data. This data is what is currently in use by the system and requires that power be present. The data does not remain when the device loses power (Harris, 2010). Due to the unchanging nature of the hard drive architecture, collection and examination methods of a computer system have changed very little. This reliability is in direct contrast to the mobile area of forensics. A legal background of digital forensics must be established before the issues facing mobile forensics can properly be discussed.

IV. EFFICIENT GENERALIZED FORENSICS FRAMEWORK FOR EXTRACTION AND DOCUMENTATION OF EVIDENCE FROM ANDROID DEVICES

This section outlines our methodology for extraction of digital evidence from Android devices:

A. Acquisition Methodology



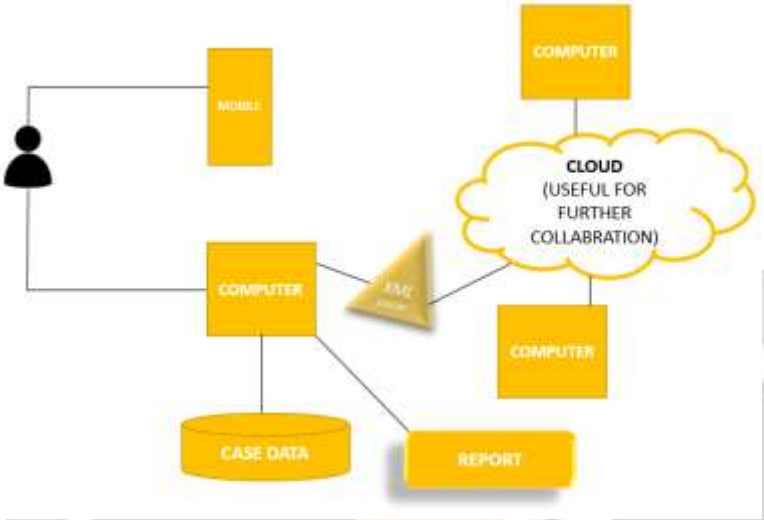
CLASSIC REMOTE ACQUISITION

The approach we propose in this paper focuses on acquiring data from Android device's internal storage memory, copying data to an external removable memory card (like SD, min SD, etc.,) as shown in Figure 3. This task of forensic acquisition of evidence can be thus performed without need

for connecting the Android device to PC. This will result in redeeming forensic operators to travel with luggage containing plenty of one-on-one tools for every single Android device [14].

B. Open Architecture

The following Figure 4 below shows the proposed architecture of Efficient Generalized Forensics Framework for Mobile Devices:



In order to acquire data from Android devices all the following components will play very vital role:

- On-Device Acquisition on SD Card
- Forensic Workstation with SD Card Reader
- Case Database
- Case Reporting Module
- Open Architecture to Collaborate with other Forensic Workstation [12].

C. Acquisition Process

The complete data acquisition process is shown in Figure 5 below:

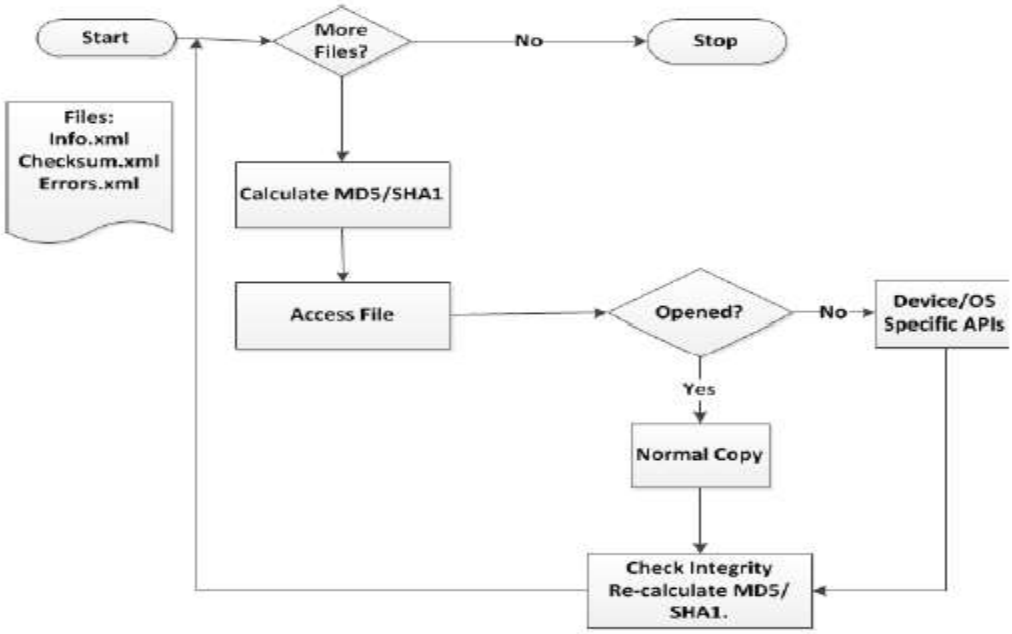


Fig. 5 Acquisition Process

Before Acquisition process starts, it is necessary to shield the device with Farady cage to avoid network communication which could trigger events resulting in modification of file system's object. Mostly all the Android devices have option to plug-in a SD card while the device is powered-on (hotplug) without removing battery. This is really helpful since for collecting data which otherwise could be altered if the device is turned off before the seizure process. Therefore, we have to check first if a SD card is already plugged, and replace it with a SD card containing updated version of Efficient Generalized Forensics Framework Acquisition App. We need to then navigate through File Explorer to launch the Acquisition App. The App will kill all non-necessary processes running on the system in order to avoid locking problems. In order to insure integrity acquired data, the App performs hashing of each file before and after copy. The relevant information about all the file hashes are saved in Checksum.xml log file for further analysis later. Data acquisition is done using Device/OS specific API's along with deleted data using file allocation table [19].

D. Acquisition Algorithm

The implementation details are provided in the following Figure 6 which shows the pseudo-code for the Acquisition Process [17]:

Input: A path p.

Output: none.

for all objects obj (files and directories) in p **do**

ifobj is a directory **then**

Create a directory named p in the SD Card

Recursively call Acquisition**(p/obj)**

else ifobj is a file **then**

Compute MD5/SHA1 hash of **obj**

Copy **obj** in path p on the SD Card

If obj has not been copied **then**

Access to obj with Device Specific APIs

If obj could be accessed **then**

Recreate a similar database in path p on the SD Card

end if

end if

end if

Compute MD5/SHA1 hash of the copied obj on the SD Card

end if

end for

The above algorithm performs following two main tasks:

 File Copy

In this task, all the files on Android device are copied onto the SD card [14].

 Hashing

This task ensures integrity of the copied files and allows discovering if some file got changed during the copy process [20].

The Acquisition Algorithm uses Android OS API's for performing various functions during the above process. This algorithm preserves the original directory structure, by copying files according to their original position recursively. The hashing ensures integrity check before and after copy of each file from Android device to the SD card data dump. The hashes are also written in Checksum.xml log file in home root directory which can be used for further verification. The Acquisition Algorithm invokes the hash function before and after copy of each file, ensuring verification of changes if any during the file copy [9].

CONCLUSION AND FUTURE WORK

Smartphones are becoming even more sophisticated and able. Both law enforcement and the private sector need to invest time and money into learning about new operating systems and developing new forensic methods. Android OS is already the most popular OS on smartphones and many more devices like tablets, televisions, vehicles, gaming devices, notebooks etc are already running on Android OS. However forensic analysis and security engineers have struggled as there is lack of knowledge and supported tools for investigating these devices. Android Forensics is a quite young and immature discipline, even more when contextualized to the Mobile Forensics. This paper outlined Efficient Generalized Forensics Framework for extraction and documentation of evidence from Android devices. This approach will ensure to acquire a complete and consistent snapshot of Android devices with through integrity verification using hashing algorithms. This study will be further used to do experimental analysis and relevant comparison with other commercial forensics tools available in market.

REFERENCES

1. Paul Doran, MDA (2008). 2008- the year of mobile customers, URL, http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_releas e_Nov07.pdf (Accessed in August 18, 2008).

2. Canalys (2007). Smart mobile device shipments hit 118 million in 2007, up 53% on 2006, URL, http://www.canalys.com/pr/2008/r2008021.htm, (Accessed in August 18, 2008).

3. Aljazeera (2005). Phone Dealers in al-Hariri Probe Net, URL, http://english.aljazeera.net/archive/2005/09/200841014558113928.html, (Accessed in August 18, 2008).

4. Westtek (2008). ClearVue Suite, URL http://www.westtek.com/smartphone/, (Accessed in August 18, 2008).

5. Alex Manfrediz (2008). IDC Press Release. IDC Finds More of the World's Population Connecting to the Internet in New Ways and Embracing Web 2.0 Activities, URL, http://www.idc.com/getdoc.jsp?containerId=prUS21303808, (Accessed in August 18, 2008).

6. FoneKey (2008). URL, www.FoneKey.net, (Accessed in August 18, 2008).

7. Ducell (2008). URL, www.DuCell.org, (Accessed in August 18, 2008).

8. Mock, D (2002). Wireless Advances the Criminal Enterprise, URL, http://www.thefeaturearchives.com/topic/Technology/Wireless_Advances_the_Criminal_Enterpris e.html, (Accessed in August 18, 2008).

9. Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2007). Cell Phone Forensic Tools: An Overview and Analysis, URL http://csrc.nist.gov/publications/nistir/nistir-7250.pdf, (Accessed in August 18, 2008).

10. Carrier, B. D. (2006). Risks of Live Digital Forensic Analysis. Communications of the ACM, 49(2), 56-61. URL, http://portal.acm.org/citation.cfm?id=1113034.1113069&coll=GUIDE&dl=GUIDE, (Accessed in August 18, 2008).

11. Jansen, W., & Ayers, R. (2004). Guidelines on PDA Forensics, URL http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf, (Accessed in August 18, 2008

12. Symbian (2008). History, URL http://www.symbian.com/about/overview/history/history.html, (Accessed in August 18, 2008).

13. Jansen, W., & Ayers, R. (2006). Guidelines on Cell Phone Forensics, URL http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf, (Accessed in August 18, 2008).

14. Zheng, P., & Ni, L. M. (2006). The Rise of the Smart Phone. IEEE Distributed Systems Online, 7(3), art. no. 0603-o3003.

15. Espiner, T. (2006). Mobile Phone Forensics 'Hole' Reported, URL http://news.zdnet.co.uk/hardware/0,1000000091,39277347,00.htm, (Accessed in August 18, 2008).

16. McCarthy, P. (2005). Forensic Analysis of Mobile Phones. Unpublished Bachelor of Computer and Information Science (Honours) Degree, University of South Australia, Adelaide.

17. Jansen, W. (2005). Mobile Device Forensic Software Tools. Paper presented at the Techno Forensics 2005, Gaithersburg, MD, USA.

18. SWGDE. (2006). SWGDE and SWGIT Digital & Multimedia Evidence Glossary, URL http://www.swgde.org/documents/swgde2005/SWGDE%20and%20SWGIT%20Combined%20M aster%20Glossary%20of%20Terms%20-July%2020..pdf, (Accessed in August 18, 2008).

19. Ghosh, A. (2004). Guidelines for the Management of IT Evidence, URL http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf, (Accessed in August 18, 2008).

20. ACPO. (2003). Good Practice Guide for Computer based Electronic Evidence, URL http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, (Accessed in August 18, 2008).