



# Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective

Rizwan Ahmed<sup>1\*</sup> and Rajiv V. Dharaskar<sup>1</sup>

## ABSTRACT

*Mobile phone proliferation in our societies is on the increase. Advances in semiconductor technologies related to mobile phones and the increase of computing power of mobile phones led to an increase of functionality of mobile phones while keeping the size of such devices small enough to fit in a pocket. This led mobile phones to become portable data carriers. This in turn increased the potential for data stored on mobile phone handsets to be used as evidence in civil or criminal cases. This paper examines the nature of some of the newer pieces of information that can become potential evidence on mobile phones. It also discusses some of the emerging technologies and their potential impact on mobile phone based evidence. The paper will also cover some of the inherent differences between mobile phone forensics and computer forensics. It also highlights some of the weaknesses of mobile forensic toolkits and procedures. Finally, the paper shows the need for more in depth examination of mobile phone evidence.*

**Keywords:** Mobile forensics, cell phone evidence, mobile phone forensic toolkits, digital device forensics

## 1. Introduction

Mobile phone proliferation is on the increase with the worldwide cellular subscriber base reaching 4 billion by the year end of 2008 (Doran, 2008). While mobile phones outsell personal computers three to one, mobile phone forensics still lags behind computer forensics. Even when comparing sales figures of smart mobile phone devices which have some Personal Digital Assistant (PDA) capabilities, to the sale figures of the actual PDA devices, smart mobile phones sales continued to grow while the PDA figures continue to decline (Canalys, 2007). Data acquired from mobile phones continues to be used as evidence in criminal, civil and even high profile cases (Aljazeera, 2005). However, validated frameworks and techniques to acquire mobile phone data are virtually non-existent.

### 1.1 The need for mobile phone handset forensics

The following section of the paper will discuss the need for mobile forensics by highlighting the following:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices

---

<sup>1</sup> G. H. Raisoni College of Engineering and Technology, Hingna Rooda, Nagpur- 440016, India

\* Corresponding Author: (E-mail : rizwanmailbox@gmail.com, Telephone: +91 9823159796)

### **1.2 Use of mobile phones to store and transmit personal and corporate information**

Mobile phones applications are being developed in a rapid pace. Word processors, spreadsheets, and database-based applications have already been ported to mobile phone devices (Westtek, 2008). The mobile phone's ability to store, view and print electronic documents transformed these devices into mobile offices. The ability to send and receive Short Message Service (SMS) messages also transformed mobiles into a message centre. In India alone, nearly 1.5 billion (1,492,400,769) text messages (SMS) were sent per week between January and May, 2008, the Mobile Data Association (MDA) said (Doran, 2008).

SMS was further upgraded to Enhanced Messaging Service (EMS) and saw some added features while the latest upgrade to Multimedia Messaging Service (MMS) added support for multimedia objects and seamless integration with email gateways that enabled users to send content rich emails using the MMS service. In India, more than 10 million (10,734,555) pictures and video messaging (MMS) were sent per week — a year on year growth of 30 percent (Doran, 2008).

Furthermore, technologies such as “push e-mail” and always-on connections added convenience and powerful communications capabilities to mobile devices. Push e-mail provided users with instant email notification and download capability, where when a new e-mail arrives; it is instantly and actively transferred by the mail server to the email client, in this case, the mobile phone. This in turn made the mobile phone an email storage and transfer tool.

Roughly 40% of all Internet users worldwide currently have mobile Internet access. The number of mobile Internet users will reach 546 million in 2008, nearly twice as many as in 2006, and is forecast to surpass 1.5 billion worldwide in 2012. Among mobile Internet users, the most popular online activities are searching the Web, accessing news and sports information, downloading music, videos, and ringtones, using instant messaging, and using Internet email. By 2012, downloading music, videos, and ringtones will become the number one activity among mobile Internet users worldwide (Manfrediz, 2008).

### **1.3 Use of mobile phones in online transactions**

Wireless Application Protocol (WAP) enabled the use of mobile phones in online transactions. Technologies such as digital wallets (E-Wallet) added convenience to online transactions using a mobile phone. Further enhancements in connectivity and security of mobile devices and networks enabled mobile phones to be used securely to conduct transactions such as stock trading, online shopping, mobile banking and hotel reservations and check-in (FoneKey, 2008) and flight reservations and confirmation (Ducell, 2008). As part of development of mobile systems, the novel idea of mobile forensics came to our mind and so this research paper is a milestone to achieve the same objectives.

### **1.4 Law enforcement, criminals and mobile phone devices**

The gap between law enforcement and organised crime is still considerable when it comes to the utilisation of mobile phone technologies. Mobile phones and pagers were used in the early 1980s by criminal organisations as a tool to evade capture as well as a means to facilitate everyday operations. Ironically, while it took decades to convince legitimate businesses that mobile connectivity can improve their operations, just about every person involved at any level of crime already knew in the early 1980s that mobile phones can provide a substantial return on investment (Mock, 2002).

On the other hand, law enforcement and digital forensics still lag behind when it comes to dealing with digital evidence obtained from mobile devices. This is partly due to some of the following reasons (Ayers, 2007):

- The mobility aspect of the device requires specialized interfaces, storage media and hardware
- The file system residing in volatile memory versus stand alone hard disk drives
- Hibernation behaviour in which processes are suspended when the device powered off or idle

but at the same time, remaining active

- The diverse variety of embedded operating systems in use today
- The short product cycles for new devices and their respective operating systems

These differences make it important to distinguish between mobile phone and computer forensics.

## **2. Computer Forensics V/s Mobile Phone Handset Forensics**

The following sections of the paper compare computer and mobile forensics in the following aspects:

- Reproducibility of evidence in the case of dead forensic analysis
- Connectivity options and their impact on dead and live forensic analysis
- Operating Systems (OS) and File Systems (FS)
- Hardware
- Forensic Tools and Toolkits Available

### ***2.1 Reproducibility of evidence in the case of dead forensic analysis***

Digital investigations can involve dead and/or live analysis techniques. In dead forensic analysis, the target device is powered off and an image of the entire hard disk is made. A one-way-hash function is then used to compute a value for both, the entire contents of the original hard disk and the forensically acquired image of the entire hard disk. If the two values match, it means that the image acquired represents a bit-wise copy of the entire hard disk. After that, the acquired image is analysed in a lab using a trusted OS and sound forensic applications. This process is referred to as offline forensic analysis or offline forensic inspection.

One of the key differences between traditional computer forensics and mobile phone forensics is the reproducibility of evidence in the case of dead forensic analysis. This is due to the nature of mobile phone devices being constantly active and updating information on their memory. One of the causes of that is the device clock on mobile phones which constantly changes and by doing so alters the data on the memory of that device. This causes the data on the mobile device to continuously change and therefore causing the forensic hash produced from it to generate a different value every time the function is run on the device's memory (Ayers, 2007). This means that it will be impossible to attain a bit-wise copy over the entire contents of a mobile phone's memory.

### ***2.2 Connectivity options and their impact on dead and live forensic analysis***

Live forensic analysis in this context refers to online analysis versus offline analysis. Online analysis means that the system is not taken offline neither physically nor logically (Carrier, 2006). Connectivity options refer to the ways in which a system or device is connected to the outside world be it a wired or wireless connection. Even though built-in connectivity options for computers are limited when compared to the increasingly developing connectivity options on mobile phone devices, connectivity options are addressed in both live and dead computer forensics. On the other hand, live analysis is not even heard of yet when it comes to mobile phone handset forensics.

### ***2.3 Operating Systems and File Systems***

Computer forensic investigators are very familiar with computer operating systems and are comfortable working with computer file systems but they are still not as familiar with working with the wide range of mobile OS and FS varieties. One of the main issues facing mobile forensics is the availability of proprietary OS versions in the market. Some of these OS versions are developed by well known manufacturers such as Nokia and Samsung while some are developed by little known Chinese, Korean and other regional manufacturers. Mobile phone operating systems are generally closed source with the exception of Linux based mobile phones. This makes developing forensics tools and testing them an onus task. Moreover,

mobile phone manufacturers, OS developers and even forensic tool developers are reluctant to release information about the inner workings of their codes as they regard their source code as a trade secret.

Another issue with mobile OS and FS when compared to computers is the states of operation. While computers can be clearly switched on or off, the same can not be said about some mobile phone devices. This is especially true for mobile phones stemming from a PDA heritage where the device remains active even when it is turned off. Therefore, back-to-back dead forensic acquisitions of the same device will generate different hash values each time it is acquired even though the device is turned off (Jansen, 2004).

A key difference between computers and mobile phones is the data storage medium. Volatile memory is used to store user data in mobile phones while computers use non-volatile hard disk drives as a storage medium. In mobile phones, this means that if the mobile phone is disconnected from a power source and the internal battery is depleted, user data can be lost. On the contrary, with non-volatile drives, even if the power source is disconnected, user data is still saved on the hard disk surface and faces no risk of deletion due to the lack of a power source. From a forensics point of view, evidence on the mobile phone device can be lost if power is not maintained on it. This means that investigators must insure that the mobile device will have a power supply attached to it to make sure data on the device is maintained.

One of the drawbacks currently facing mobile OS and FS forensic development is the extremely short OS release cycles. Symbian, a well known developer of mobile phone operating systems is a prime example of the short life cycle of each of its OS releases. Symbian produces a major release every twelve months or less with minor releases coming in between those major releases (Symbian, 2008). This short release cycle makes timely development, testing and release of forensic tools and updates that deal with the newer OS releases difficult to achieve.

#### **2.4 Hardware**

Mobile phones are portable devices that are made for a specific function rather than computers which are made for a more general application. Therefore, mobile phone hardware architecture is built with mobility, extended battery life, simple functionality and light weightiness in mind. This makes the general characteristics of a mobile phone very different from a computer in the way it stores the OS, how its processor behaves and how it handles its internal and external memory.

The hardware architecture of a typical mobile phone usually consists of a microprocessor, main board, Read Only Memory (ROM), Random Access Memory (RAM), a radio module or antenna, a digital signal processor, a display unit, a microphone and speaker, an input interface device (i.e., keypad, keyboard, or touch screen) and a battery. The OS usually resides in ROM while RAM is generally used to store other data such as user data and general user modifiable settings. The ROM may be re-flashed and updated by the user of the phone by downloading a file from a web site and executing it on a personal computer that is connected to the phone device.

This general architecture does not apply to all models of mobile phones as mobile phones are very diverse in hardware architecture and OS varieties (Jansen, 2006). Some mobile devices might contain additional devices and modules such as a digital camera, Global Positioning device (GPS), wireless and network modules, and even a small hard disk. Manufacturers highly customize operating systems to suit their hardware devices and the feature sets they want to support on them (Zheng, 2006). This means that a certain version of an OS on a certain manufacturer's phone model does not mean that the same version of the same OS on a different manufacturer's hardware will be exactly the same. This is true also for on the same manufacturer's phones with different hardware architectures. Moreover, ROM updates are not only OS specific but are also hardware specific. Also, some phone providers add functionality and customization options to their ROMs which mean that the same version phone of a phone purchased from two different

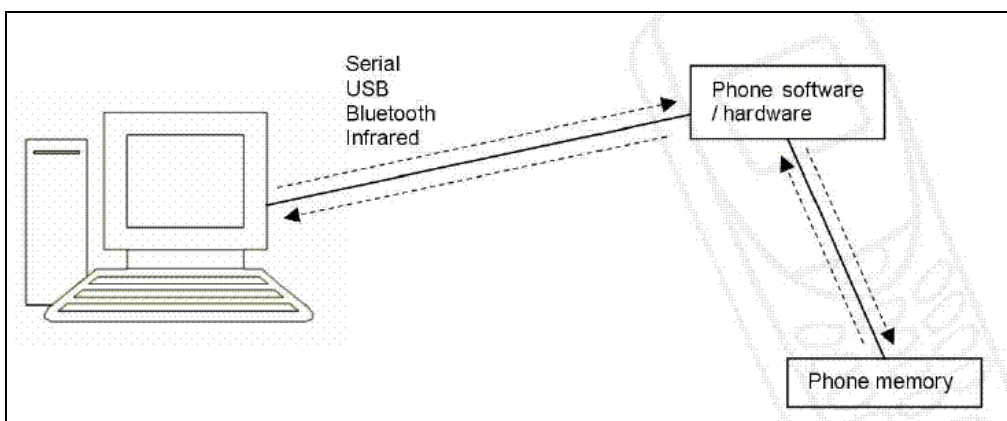
providers might not be exactly the same.

Proprietary hardware is another issue facing mobile phone forensics. Support for such devices is not available from mobile forensics tools. About 16% of mobile phones in the market today come from proprietary manufacturers and are not supported by forensic tools (Espiner, 2006). Moreover, some manufacturers produce mobile phones that have no interfaces that are accessible through a computer. This makes forensically acquiring those mobile phones harder to achieve if not impossible.

The wide array of connection socket and cable types for connecting a mobile phone to a computer makes identifying the right cable for the right phone model an onus task for the forensic investigator. Phone chargers also come in different shapes, sizes and socket types and make identifying the right charger for the right model a hard task for the investigator. Short product cycles also contribute to the difficulty in dealing with mobile phones forensically. Support for newer models by forensic tools is usually slow. The following section discusses in more detail some of the mobile forensic tools and their features and drawbacks when compared to computer based forensic tools.

### 2.5 Forensic Tools and Toolkits Available

Early mobile phones did not have the capacity to store large amounts of information so law enforcement officers did not need to access mobile phone handsets to get information on a suspect. The focus was more on phone records from the telecommunications companies. Nowadays, mobile phones have large storage capacity and a wide array of applications and connectivity options besides connectivity with the telecommunications provider. Mobile phone forensic tools and toolkits are still immature in dealing with these advances in mobile phone technology. Mobile forensic toolkits are developed by third party companies and the toolkits are not independently verified or tested for forensic soundness. The developers of the toolkits admit to using both, manufacturer supplied and self developed commands and access methods to gain data access to memory on mobile devices (McCarthy, 2005). The tools often limit themselves to one or more phone manufacturer handsets with a limited number of devices supported. Some of the tools are also limited when it comes to connectivity options when it comes to acquisition of data from the handset. For example, some tools are limited to wired connections as opposed to Infrared (IrDA) and Bluetooth access to data on mobile devices. Moreover, while some toolkits provide acquisition capabilities, they do not provide examination or reporting facilities (Jansen, 2005). Moreover, direct access to data on the mobile phone is not achievable. Phone software and/or hardware must be used to acquire data from the mobile phone's memory as shown in Figure 1:



**Figure 1:** Indirect Access to Data in Mobile Phone Memory via Software and Hardware Commands and Methods (McCarthy, 2005).

This inherent difference between computer forensics and mobile phone forensics affects how data acquired from mobile phones is perceived. To make this data trustworthy, independent evaluation of mobile forensic tools has to become an integral part of their development. The only currently available tools evaluation document for mobile phone forensics is published by the National Institute of Standards and Technology (NIST) in the United States (Ayers, 2007). The document evaluated eight mobile phone forensic toolkits. It covered a range of devices from basic to smart phones. It showed that none of the forensic toolkits supported all the mobile phone devices covered in the document. The document however limited its scope to a set of scenarios with a definite set of prescribed activities that were used to gauge the capabilities of each of the eight toolkits evaluated. The document also tested the toolkits in one set of conditions which was a virtual machine installed on a windows machine. This insured toolkit segregation and ruled out the possibility of conflicts amongst the tools (Jansen, 2006).

### **3. Mobile Phone Data as Evidence**

This section of the paper will highlight some forensic definitions, principles and best practice guidelines and how they address mobile phone forensics issues. It will also discuss some of the forensic guides that cover mobile phone forensics and mention their shortcomings.

#### ***3.1 Definition of Digital Evidence***

According to the Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence (SWGDE, 2006) is “information of probative value that is stored or transmitted in binary form”. Therefore, according to this definition, evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices. Furthermore, digital evidence is not only limited to traditional computer crimes such as hacking and intrusion, but also extends to include every crime category in which digital evidence can be found (Ghosh, 2004). However, the Australian Standards HB171 document titled “Guidelines for the Management of IT Evidence” refers to IT Evidence as: “any information, whether subject to human intervention or otherwise, that has been extracted from a computer. IT evidence must be in a human readable form or able to be interpreted by persons who are skilled in the representation of such information with the assistance of a computer program”. This definition is lacking as it does not address evidence on digital devices other than a computer (Ghosh, 2004). The latter definition shows that not all digital evidence definitions or procedures related to them are updated to address mobile phone evidence. Even the Information Technology Act 2000 (No. 21 of 2000) is not updated to include information about mobile phone evidence (Yahoo News India, 2008). This fact again can be clearly highlighted in view of two big criminal cases (Helplinelaw, 2007) in India which involved mobile phone evidence. The following section of the paper will cover some of these definitions and procedures and highlight their shortcomings.

#### ***3.2 Principles of Electronic Evidence***

According to the United Kingdom’s Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence, Four principles are involved with Computer-Based Electronic Evidence (ACPO, 2003). They are:

- Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation (the case officer) has overall responsibility

for ensuring that the law and these principles are adhered to.

ACPO's guide regards computer based electronic evidence as no different from documentary evidence and as such is subject to the same rules and laws that apply to documentary evidence (ACPO, 2003). The ACPO guide also recognized that not all electronic evidence can fall into the scope of its guide and gave an example of mobile phone evidence as evidence that might not follow the guide. It also mentioned that not following the guide does not necessarily mean that the evidence collected is not considered as viable evidence.

However, Principle 1 of the ACPO guide can not be complied with when it comes to mobile phone forensics. This is because mobile phone storage is continually changing and that may happen automatically without interference from the mobile user (Jansen, 2004). Thus, the goal with mobile phone acquisition should be to affect the contents of the storage of the mobile as less as possible and adhere to the second and third principles that focus more on the competence of the specialist and the generation of a detailed audit trail (Jansen, 2004). In adhering with Principle 2, the specialist must be competent enough to understand both the internals of both hardware and software of the specific mobile device they are dealing with as well as have an expert knowledge of the tools they are using to acquire evidence from the device.

More than one tool is recommended to be used when acquiring evidence from mobile phone as some tools do not return error messages when they fail in a particular task (Jansen, 2004). When it comes to adhering with Principle 3, providing a thorough record of all processes used to obtain the evidence in a way that can be duplicated by an independent third party is essential in order for the evidence gathered to be admissible in court.

When it comes to the recovery of digital Evidence, "The Guidelines for Best Practice in the Forensic Examination of Digital Technology" publication by the International Organization on Computer Evidence (IOCE) considers the following as the General Principles Applying to the Recovery of Digital Evidence (IOCE, 2002):

- The general rules of evidence should be applied to all digital evidence.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

As with the ACPO principles, principle B can not be strictly applied to evidence recovered from Smartphone devices because of their dynamic nature. Furthermore, mobile phone acquisition tools that claim to be forensically sound do not directly access the phone's memory but rather use commands provided by the phone's software and/or hardware interfaces for memory access and thus rely on the forensic soundness of such software or hardware access methods (McCarthy, 2005). Therefore, when using such tools, the ability to extract that information in a manner that will not significantly change the mobile phone's memory is not verifiable.

### ***3.3 Mobile Phone Evidence Guides***

There are a number of guides that briefly mention potential evidence on mobile phone devices. In this section, some of these guides will be highlighted and their shortcomings explained. The Best Practices for Seizing Electronic Evidence published by the United States Secret Service (USSS) referred to mobile

phones as “Wireless Telephones” under the “Other Electronic Storage Devices” heading (USSS, 2006). The National Institute of Justice (NIJ), which is under the United States Department of Justice lists mobile phones under the heading of “Telephones” in their “Electronic Crime Scene Investigation: A guide for First Responders” publication (NIJ, 2001). Both of the guides do not provide sufficient details on how to forensically approach smart phones. This might be in part because these guides are outdated. Both guides however mention that mobile phones might have some potential evidence on them. The extent of the coverage is very limited and does not address smart phone storage capabilities and applications on them. The USSS document also lists a set of rules on whether to turn on or off the device (IOCE, 2002):

- If the device is "ON", do NOT turn it "OFF".
- Turning it "OFF" could activate lockout feature.
- Write down all information on display (photograph if possible).
- Power down prior to transport (take any power supply cords present).
- If the device is "OFF", leave it "OFF".
- Turning it on could alter evidence on device (same as computers).
- Upon seizure get it to an expert as soon as possible or contact local service provider.
- If an expert is unavailable, USE A DIFFERENT TELEPHONE and contact 1-800-LAWBUST (a 24 x 7 service provided by the cellular telephone industry).
- Make every effort to locate any instruction manuals pertaining to the device.

On the other hand, the NIJ guide for first responders lists the following as potential evidence (NIJ, 2001): Appointment calendars/information., password, caller identification information, phone book, electronic serial number, text messages, e-mail, voice mail, memos, and web browsers. The guide however failed to mention that mobile devices could have external storage attached to them even though it mentioned that other equipment such as fax machines may contain such external storage devices. It did however emphasize that miscellaneous electronic items such as cellular phone cables and cloning equipment may contain information of evidentiary value.

Both guides fail to mention that mobile phones could have electronic documents, handwriting information, or location information on them. The guides also fail to mention that phone based applications such as Symbian, Mobile Linux and Windows Mobile applications could have evidential significances. Both, Symbian and Windows Mobile based phones were found to execute malicious code such as Trojans and viruses especially ones transferred via Bluetooth technology (McCarthy, 2005) (Keizer, 2006). Non malicious applications on mobile phones could also be considered as evidence as they might be used to conduct illegal activities or can have log files or data that can be considered as evidence. Therefore all phone applications and data related to them should be considered as potential evidence. This includes logs relating Bluetooth, Infrared (IrDA), Wi-Max and Wi-Fi communications and Internet related data such as instant messaging data and browser history data. Java applications should also be considered as evidence as many mobile phone operating systems support a version of Java (McCarthy, 2005).

When it comes to handling instructions for mobile phones, the United Kingdom’s Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence lists the following instructions (CCIPS, 2002):

- Handling of mobile phones:
- Any interaction with the handset on a mobile phone could result in loss of evidence and it is important not to interrogate the handset or SIM.
- Before handling, decide if any other evidence is required from the phone (such as DNA/fingerprints/drugs/accelerants). If evidence in addition to electronic data is required, follow the general handling procedures for that evidence type laid out in the Scenes of Crime Handbook or contact the scenes of crime officer.
- General advice is to switch the handset OFF due to the potential for loss of data if the battery fails or new network traffic overwrites call logs or recoverable deleted areas (e.g. SMS); there is also

potential for sabotage. However, investigating officers (OIC) may require the phone to remain on for monitoring purposes while live enquiries continue. If this is the case, ensure the unit is kept charged and not tampered with. In all events, power down the unit prior to transport.

Note that the on/off rules here initially conflict with the USSS guide but both guides agree to turn off the device before transport. The ACPO guide contains flowcharts when it comes to seizure of electronic evidence and PDAs which may not be applied to mobile phone devices. The charts are included in the Appendix section as a reference only. An updated chart for examining mobile phones by NSLEC in the U.K. contains references to the appropriate action to be taken when seizing a mobile phone and whether it was turned on or off when it was seized (Mellars, 2004). The chart is in no way all-inclusive as it refers to only three types of evidence from mobile phones and they are SMS messages, voicemail and address book/call history details. The guidelines and procedures need to be continually updated to cater for future trends in mobile phones. Some of these trends are mentioned in the next section.

## **4. Future Trends**

Future trends in mobile phone devices and their components can be divided to processor speed and components, battery types and technologies affecting them, and finally, memory and storage capacities. All of these components and their developments may have an impact on mobile device forensics.

### ***4.1 Processor Components and Speed***

Intel has already demonstrated a 1GHz processor for mobile devices (Zheng, 2006). In addition to this high processing speed, smart mobile phone devices are showing the trend of using System on Chip (SoC) technology. This technology allows the processor to incorporate a set of distinct functionalities in the same package which reduces the number of chips required by it as well as incorporating a considerable amount of built-in memory (Jansen, 2006). This change in processor architecture may have an undesirable impact on mobile forensics.

### ***4.2 Battery Life***

Mobile phones typically use three types of batteries: NiMH (nickel metal hydride), Li-ion (lithium-ion), and Li-polymer. Toshiba announced that it will be releasing a lithium-ion battery technology that will allow batteries to recharge sixty times faster than conventional batteries which means that it will take about a minute for a battery to go from drained to an 80% charge (Becker, 2005). Other battery types such as fuel cell batteries have emerged but are not yet available in mass production. Wireless communications such as the use of Wi-Fi, Wi-Max, and Bluetooth will drain batteries much more rapidly than simple computing tasks and this will present battery manufacturers with more challenges as these communication and connectivity options are becoming more natively integrated into today's smart phones. Battery life can have a huge impact on a mobile forensic investigation as volatile data can be lost if the battery is drained.

### ***4.3 Memory and Storage***

Mobile phone's OS and applications are smaller in size than computer based OS and applications. Therefore, it makes more sense to store them in RAM, ROM or flash memory. Current high end mobile phones may have 64 to 128 MB of static RAM for application code, 128 to 256 MB of flash memory for system code, and more than 128 MB of flash memory for user data (Zheng, 2006). The amount of RAM, ROM or flash memory is on the rise which means also that data access and transfer rates to support them will improve.

Advances in technologies and circuitry enabled external memory support to become main stream in higher end mobile phones. The physical sizes of such devices is declining while their storage capacities rising. The reduction of size has also made these devices very fragile and easily concealable by evildoers. Moreover,

some mobile phones support the swapping of external storage memory in and out without turning off the mobile device or taking out the battery cover. Auditing such devices on the mobile OS level must be addressed for mobile forensic reasons.

## 5. Concluding Remarks

With increased connectivity options and higher storage capacities and processing power, abuse of mobile phones can become more main stream. Mobile phones outsell personal computers and with digital crime rates rising, the mobile phone may be the next avenue for abuse for digital crime. Mobile phones with their increased connectivity options may become a source of viruses that infect computers and spread on the internet. Virus writers typically look for operating systems that are widely used. This is because they want their attacks to have the most impact. When it comes to mobile phones and their operating systems, there seems to be certain operating systems that are dominating the market which makes them a prime candidate for attacks. According to recent studies, phone virus and malware infection rates are expected to increase with newer smart phones (Long, 2005) (McAfee Mobile Security Report, 2008).

Mobile phone technology is evolving at a rapid pace. Digital forensics relating to mobile devices seems to be at a stand still or evolving slowly. For mobile phone forensics to catch up with release cycles of mobile phones, more comprehensive and in depth framework for evaluating mobile forensic toolkits should be developed and data on appropriate tools and techniques for each type of phone should be made available a timely manner. In order to accomplish this, the authors are further developing an open source “MFL3G: Mobile Forensics Library” based on methodologies identified in the paper.

## 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\\_release\\_Nov07.pdf](http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_release_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](http://www.FoneKey.net), (Accessed in August 18, 2008).
7. Ducell (2008). URL, [www.DuCell.org](http://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\\_Enterprise.html](http://www.thefeaturearchives.com/topic/Technology/Wireless_Advances_the_Criminal_Enterprise.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%20aster%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](http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf), (Accessed in August 18, 2008).
  21. IOCE. (2002). *Best Practice Guidelines for Examination of Digital Evidence*, URL <http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf>, (Accessed in August 18, 2008).
  22. USSS. (2006). *Best Practices for Seizing Electronic Evidence*, URL [http://www.ustreas.gov/ussse/electronic\\_evidence.shtml](http://www.ustreas.gov/ussse/electronic_evidence.shtml), (Accessed in August 18, 2008).
  23. NIJ. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*, URL <http://www.ncjrs.gov/pdffiles1/nij/187736.pdf>, (Accessed in August 18, 2008).
  24. Keizer, G. (2006). *First Mobile Phone Java Trojan on the Loose*, URL <http://www.crn.com.au/story.aspx?CIID=35467&r=rstory>, (Accessed in August 18, 2008).
  25. CCIPS. (2002). *Searching and Seizing Computers and Related Electronic Evidence Issues*, URL <http://www.usdoj.gov/criminal/cybercrime/searching.html>, (Accessed in August 18, 2008).
  26. Mellars, B. (2004). *Forensic Examination of Mobile Phones*. *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, 1(4), 266-272.
  27. Becker, D. (2005). *Toshiba Reports Battery Breakthrough*, URL [http://news.com.com/2061-10786\\_3-5649141.html?tag=nl](http://news.com.com/2061-10786_3-5649141.html?tag=nl), (Accessed in August 18, 2008).
  28. Long, M. (2005). *Airborne Viruses: Real Threat or Just Hype*, URL, [http://www.newsfactor.com/story.xhtml?story\\_id=12100002P4HM](http://www.newsfactor.com/story.xhtml?story_id=12100002P4HM), (Accessed in August 18, 2008).
  29. McAfee Mobile Security Report (2008). <http://www.mcafee.com/mobile>, (Accessed in August 18, 2008).
  30. The Information Technology Act 2000, India (2000). URL, <http://www.legalserviceindia.com/cyber/itact.html>, (Accessed in August 18, 2008).
  31. Yahoo News India (2008). *The Arushi Murder Case: CBI says it has found the evidence*. URL, [http://in.news.yahoo.com/32/20080731/1053/tnl-aarushi-case-cbi-says-it-has-found-e\\_1.html](http://in.news.yahoo.com/32/20080731/1053/tnl-aarushi-case-cbi-says-it-has-found-e_1.html), (Accessed in August 18, 2008).
  32. Helplinelaw (2007). *Pramod Mahajan Murder Trial: SMS cannot be valid evidence, says defence*. URL, <http://news.helplinelaw.com/1207/echo12.php>, (Accessed in August 18, 2008).

### **About the Authors**

*Rizwan Ahmed* has done B. E. in Computer Science and Engineering from SSGMCE, Amravati University, M. S. in Software Systems from Birla Institute of Science and Technology (BITS), Pilani, and he is currently pursuing his M. Tech in Computer Science and Engineering from G. H. Raisoni College of Engineering, Nagpur University. He has around 8 years of teaching, software development, research and consultancy experience. He currently provides his research consultancy service to IT MNC's which based out in India, specially in Nagpur. He has authored and presented more than 30 research papers in International Journals, International Conferences and National Conferences. His research interests are *Genetic Algorithms, Genetic Programming, Software Engineering, Network Security, E-Learning and M-Learning, Computer and Mobile Forensics*. He is the member of ISTE and IEEE. He has won several best research paper awards for presentations during conferences. He has recently won the coveted "Microsoft's Heroes Happen Here Contest 2008" and was adjudged with "Technology Hero" award in India from top 10,000 IT developers from around the world.

*Rajiv Dharaskar* is presently working as Professor at Department of Computer Science and Engineering, G. H Raisoni College of Engineering, Nagpur, Maharashtra. He has received Ph.D. Degree (Computer Science & Engineering, Faculty of Engineering & Technology) from Amravati University, M. Tech. (Computers) from I.S.M. and P.G. Dip., M.Phil., M.Sc. from Nagpur University. He is having 24 years of teaching and 18 years of R&D experience in the field of Computers & IT. He is an author of number books on Programming Languages. He has been actively involved in the research on Mobile Computing, Multimedia, Software Engineering, Web Technology, E-Learning and Networking. He has authored 39 research papers at various International / National Conferences and Journals. His research work has been accepted at IEEE Computer Society of USA, Bristol (UK), Hong Kong (China) etc. He has been invited as a Keynote Speaker, Invited Speaker, and Session Chair for more than 30 International & National Conferences.