Smartphone Forensic Investigation Process Model

Archit Goel *writetoarchit@gmail.com*
Student, B Tech
Northern India Engineering College, GGSIPU
New Delhi, 110053, INDIA

Anurag Tyagi *tyagi_anurag@ymail.com*
Student, B Tech
Northern India Engineering College, GGSIPU
New Delhi, 110053, INDIA

Ankit Agarwal *cs.ankit11@gmail.com*
Asst Prof
Northern India Engineering College, GGSIPU
New Delhi, 110053, INDIA

Abstract

Law practitioners are in an uninterrupted battle with criminals in the application of digital/computer technologies, and these days the advancement in the use of Smartphones and social media has exponentially increased this risk. Thus it requires the development of a sound methodology to investigate Smartphones in a well defined and secured way. Computer fraud and digital crimes are growing rapidly and only very few cases result in confidence. Nowadays Smartphones accounts for the major portion as a source of digital criminal evidence. This paper tries to enlighten the development of the digital forensics process model for Smartphones, compares digital forensic methodologies, and finally proposes a systematic Smartphone forensic investigation process model. This model adapt most of the previous methodologies with rectifying shortcomings and proposes few more steps which are necessary to be considered to move with the advancement in technology.

This paper present an overview of previous forensic strategies and the difficulties now being faced by the particular domain. The proposed model explores the different processes involved in the forensic investigation of a Smartphone in the form of an fourteen- stage model. The Smartphone forensic investigation process model (SPFIPM) has been developed with the aim of guiding the a effective way to investigate a Smartphone with more area of finding the potential evidence.

Keywords: Smartphone, Forensic, Digital Evidence.

1. INTRODUCTION

Due to advancements in technologies, mobile communication devices and Personal Digital Assistants (PDAs), such as the iPhone and Blackberry, are now not limited to making voice calls only, instead they are used for browsing the Internet and accessing emails in plethora, and as the technology is progressing, it is becoming cheaper, thereby easily available and accessible to more and more people. Although the amount of data stored in such devices is much less as compared to the amount of data stored in computers, but this small amount of data can be of

great use and is potent of revealing useful information, and thus forensic examinations of mobile communication devices can be extremely fruitful.

Digital evidence, which is defined as "*Digital evidence or electronic evidence is any probative information stored or transmitted digitally and a party to a judicial dispute in court can use the same during the trial*", can be found in memory modules and data storage areas of mobile telephones. These evidence can prove an important part of a criminal or civil prosecution. Deleted text messages can be recovered, which can reveal not only purposes and objectives but also suspect's plan of action. Billing records can put light over people close to suspect and his/her associates. Physical movement of a handset can be plotted to illustrate where a suspect may have moved to and from over a period of time, by cell site analysis.

As different mobile devices are built differently, specialized forensic techniques are required to ensure that mobile telephone forensics assessments conducted are done so in a forensically sound mode and that the information extracted will endure the inquiry of a court of law.

1.1 Why Smartphone forensics?

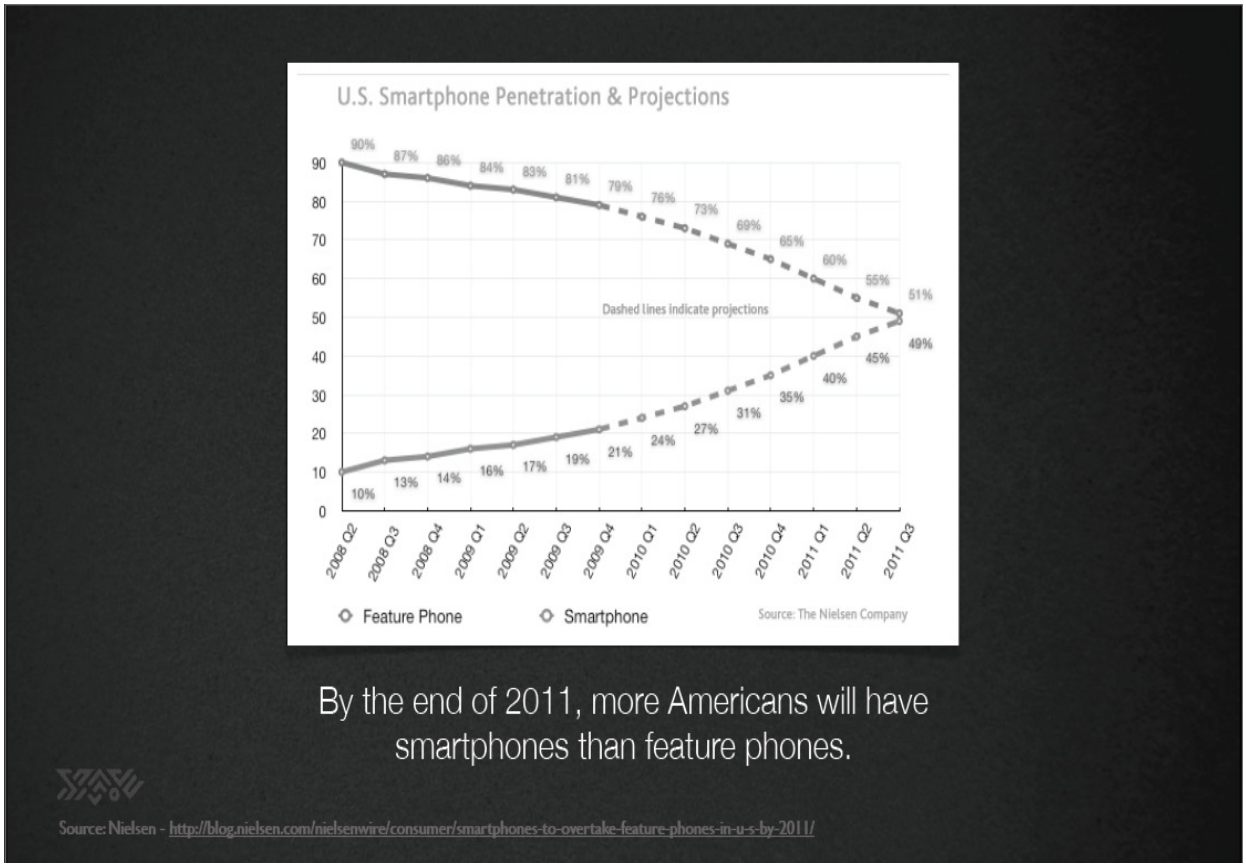

FIGURE 1: U.S. Smartphone Penetration and Projection

The following section of the paper will discuss the necessity of mobile device forensics by weighing the following:

- Use of mobile phones to amass and broadcast personal and community information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices

1.2 Use of Smartphones to amass and broadcast personal and community information.

The evolution of mobile phone applications like Word processors, Spreadsheets, and database-based applications have transformed these devices into mobile offices with ability to store, view, edit and print electronic documents. The ability to send and receive Short Message Service (SMS) messages has transformed mobiles into a message centre. The average teenager sends 3,339 texts per month [1].The facility of Multimedia Messaging Service (MMS) in mobile phones has provided support for multimedia objects and seamless amalgamation with email gateways that enables users to send content rich emails using the MMS service. Moreover, further expediency and robust, reliable, user friendly and powerful communications capabilities are induced in mobile devices with development of technologies such as "push e-mail" and always-on connections. With Push e-mail mobile device users can access their emails at any instant, anywhere as soon as email notification arrives, using their mobile device as mail client and making it an email storage and transfer tool. Popularity of Smartphones has given this trend a whole new direction.com Score said that the July 2011 US Smartphone audience reached 82.2 million people. Morgan Stanley Research estimates that sales of Smartphones will exceed those of PCs in 2012.The Coda Research Consultancy predicts global Smartphone sales of some 2.5 billion over the 2010-2015 period, and also suggests that mobile Internet use via Smartphones will increase 50 fold by the end of that period.MS Research expects 420 million Smartphones to sell in 2011 or 28% of the mobile handset market. They predict this figure will rise to over 1 billion in 2016 (half the market).

15-25 year olds spend more than 3 hours per day on their Smartphones and 60% of this is on entertainment & browsing[2]. Data usage for 3G users is almost 44% more than 2G users.IDC (December 2009) estimates there were more than 450 million mobile Internet users worldwide in 2009; this will pass the 1 billion mark by 2013.

Nielsen Informate Mobile Insights, as the alliance is called, revealed in its most recent study that the average Smartphone user spends 2 and a half hours a day using their phones with 72% of their time spent on activities such as gaming, entertainment, apps and internet related content. Only 28% of their time is now used for voice calls and text messaging.

	15-24 years	**31 years**
Total Time spent on the Smartphone	**3 hrs**	**2 hrs**
Total Time spent on Browsing & Entertainment	**2 hrs**	**1 hr**
Total Time spent on Chat & SMS	**31mns**	**15mns**

Table 1: Time spent and activities on Smartphones
Source: Nielsen Informate Mobile Insight

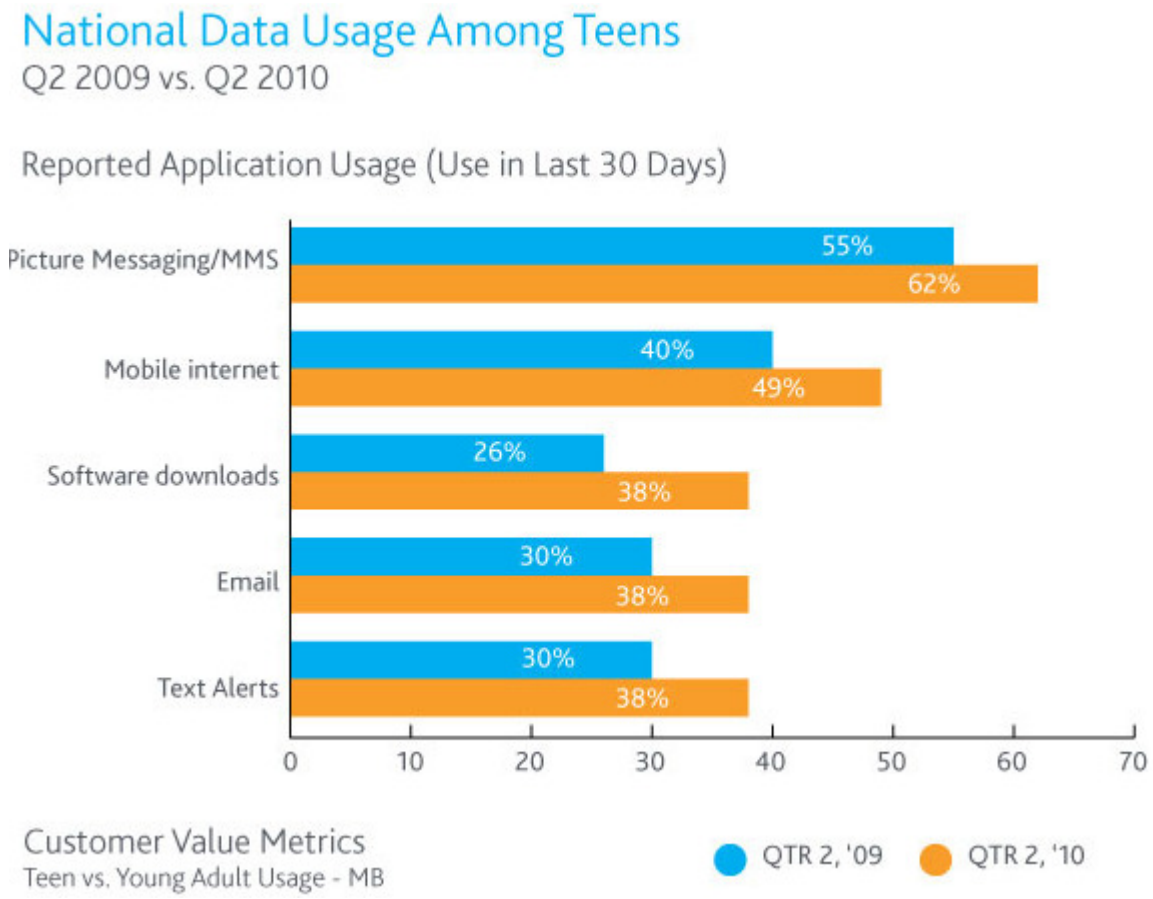

FIGURE 2: Data usage among teens
Source: Nielsen informate Mobile Insights

1.3 Use of mobile phones in online transactions

With help of Wireless Application Protocol (WAP) and technologies like digital wallets (E-Wallet) mobile phones can be used in online transactions conveniently. With 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, hotel reservations and check-in [3] and flight reservations and confirmations [4]. Jeff Bezos, founder and CEO of Amazon.com(July 2010) stated that "In the last twelve months, customers around the world have ordered more than US$1 billion of products from Amazon using a mobile device" .Global Industry Analysts(GIA) (February 2010) predicts the global customer base for m-banking will reach 1.1 billion by the year 2015. Yankee Group (June 2011) predicts that there will be 500 million m-banking users globally by 2015. Currently, 27 percent of all survey respondents use mobile banking--far more than use m-commerce (13 percent), mobile coupons (11 percent) and mobile payments (9 percent).

1.4 Law enforcement, criminals and mobile phone devices

The focus on utilization of mobile phone technologies for controlling organized crimes involving usage of such technologies in one way or the other and thereby enforcing laws is surprisingly low. Mobile phones are continually used by criminals as a means to assist everyday operations and

planning from a long time back. sardonically, while it took decades to convince lawful 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 offer a considerable return on investment [5].On the other hand, due to some of the following reasons [6], law enforcement and digital forensics still lag behind when it comes to dealing with digital evidence obtained from mobile devices:

- The mobility facet of the device requires dedicated interfaces, storage media and hardware.
- The file system residing in volatile memory versus stand alone hard disk drives.
- Hibernation behavior 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.
- The evolving use of cloud is enabling to hide the presence of data form mobiles into web.

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 evaluate mobile and computer forensics in the following aspects:

- Reproducibility of proofs in the case of dead forensic analysis
- Dead and live forensic analysis and their dependencies on connectivity options
- File systems (FS) and Operating systems (OS)
- Hardware variations
- Forensic technologies and tool-kits available

2.1 Reproducibility of proofs in the case of dead forensic analysis

In dead forensic analysis, an image of the entire hard disk is made after powering off the target device. The entire data of the original hard disk and the forensically acquired image of the entire hard disk is then computed using a one-way-hash function. This hash function generates a value for content of both, the original hard disk and the image of hard disk. The acquired image represents a bit-wise copy of the entire hard disk if the two values match. Then, sound forensic techniques are applied to analyze the acquired image in a lab using a trusted OS. This process is referred to as offline forensic analysis or offline forensic inspection.

A major distinction between conventional computer forensics and mobile phone forensics is the reproducibility of proofs in the case of dead forensic analysis. This is because mobiles, unlike traditional computers, remain active constantly and their content is continuously updated. The ever changing device clock in smart phones alters content of its memory constantly. Thus the forensic hash produced from such devices generates a different value every time the function is run on the device's memory [6]. This makes it impossible to obtain a bit-wise copy of whole data of a smart phone's memory.

2.2 Dead and live forensic analysis and their dependencies on connectivity options

Online analysis(Live analysis) means that the system is not taken offline neither physically nor logically [7]. The ways in which a device is connected to the outside world refers to the connectivity options. The connection may be wired or wireless. Although, connectivity options on smart phones are much more than those on traditional computers and are further evolving at a great rate, nothing noteworthy in field of live analysis has been done when it comes to smart phone handset forensics.

2.3 File systems (FS) and Operating systems (OS)

Digital forensic investigator have sound knowledge of computer operating systems but their knowledge and abilities to analyze digital evidences present in mobile phones is are very limited due to lack of knowledge about and familiarity with operating systems and file systems of mobile devices. Earlier, one of the main issues facing mobile forensics was the availability of proprietary OS versions in the market. Some of the OS versions were developed by well known manufacturers such as Nokia and Samsung while some were developed by little known Chinese, Korean and other regional manufacturers. This made developing forensics tools and testing them an onus task. Nowadays, as sales of Smartphones is peaking, most of which are produced by well known manufacturers like Apple, Google and RIM. This eases the scenario a bit as Apple and RIM devices use a specific OS and other mobile device manufacturers also use OS like Android by Google.

Now, the problem in developing efficient and reliable forensic analysis techniques is because the 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 cannot 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 [8]

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. 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 variations

As Smart phones are portable devices and have a specific set of functionalities unlike the large general purpose computers, the hardware architecture of smart phones is significantly different from that of computers. Thus the common characteristics of a smart phone vary from those of a computer in the way it stores the OS, its processor functions and behaves and it handles its memory(both internal and external).

The typical hardware architecture of a smart phone typically 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 is generally stored in ROM, which may be re-flashed and updated by the user of the phone by downloading a file from web and executing it on a personal computer that is connected to the phone device. These ROM updates may be hardware specific or OS specific. Other user data and settings are stored in RAM.

Some smart phones might include supplementary devices and modules like a digital camera, Global Positioning device (GPS), and even a small hard disk. OS is highly customized by manufacturers to fulfill user demands and to suit their hardware devices [9]. Thus different hardware devices may have different OS versions and specifications even if the two devices are fairly similar to each other, the same is applicable for two different(in terms of hardware) devices manufactured by a same manufacturer. Various phone providers may customize some options in device's ROMs, this causes variations to occur between two identical phones purchased from different providers. Proprietary hardware is a further concern for smart phone forensics. Mobile forensic tools hardly provide any support for such devices. About 16% of mobile phones in the market today come from proprietary manufacturers and are not supported by forensic tools. Furthermore, several smart phones have an interface which can not accessible through a computer. IN such cases forensic analysis of the device becomes even harder.

Another major factor which hinders use of existing forensic tools and presents challenges for new forensic tools under development is the small product cycle. Smart phones get out dated and out of use so rapidly that continually building forensic tools fit for newer device type is a uphill task.

2.5 Forensic technologies and tool-kits available

Earlier as mobile phones had very limited functionalities and a very limited information storage capacity, the focus was more on phone records from the telecommunications companies rather than the analysis of the device itself. But, today smart phones have large memories, loads of functionalities and applications, and many connectivity options. Mobile phone forensic tools and toolkits are not as advanced as required to match up the growth in mobile phone devices. These forensic tools are developed by third party companies and are rarely tested and verified using any sound methodology. 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 [10]. One such tool supports a very limited number of devices. Also, the extent of information a tool can extract varies and is generally quiet limited. Moreover, while some toolkits provide acquisition capabilities, they do not provide examination or reporting facilities [8]. Furthermore, direct access to information on the smart phone is not always attainable. Phone software and/or hardware must be used to obtain data from the smart phone's memory as shown in Figure:

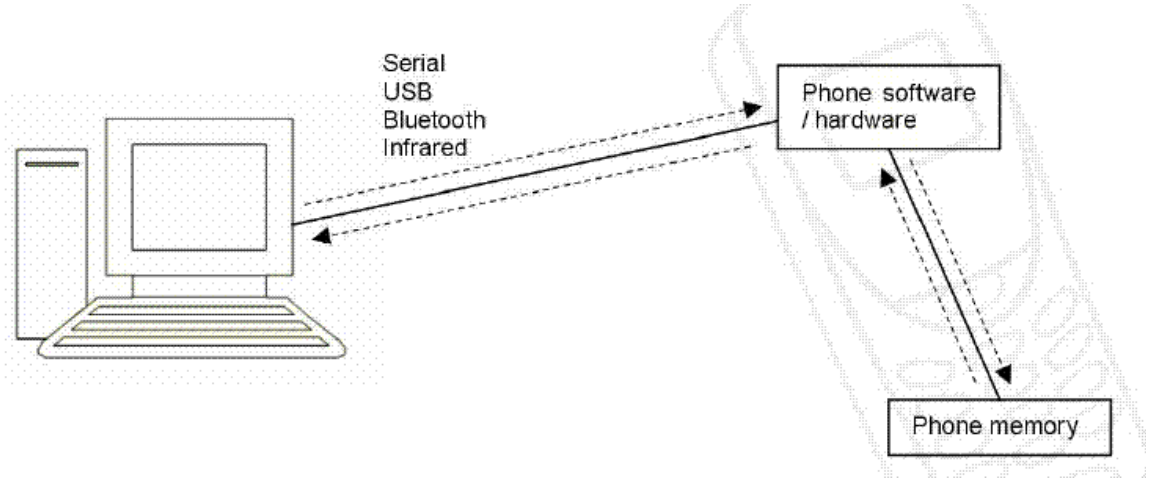

Figure 3: Indirect Access to Data in Mobile Phone Memory via Software and Hardware Commands and Methods [10].

To make this data trustable, evaluation of mobile forensic tools becomes a fundamental component of their development process Today, only a single tools evaluation document is available for mobile phone forensics and it is published by the National Institute of Standards and

Technology (NIST) in the United States [6]. Eight mobile phone forensic toolkits are evaluated in the document. A variety of devices from basic to smart phones are covered in the document. The document agreed on the state that no toolkit is available for successful forensic analysis of all mobile phone devices. But the document restricted its scope to a set of scenarios with a specific set of given activities that were used to estimate the capabilities of each of the eight toolkits under evaluation. Also, the document 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 [8].

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. In this section, some of the forensic guides that address mobile phone forensics are discussed and their shortcomings or flaws are mentioned.

3.1 Definition of Digital Evidence

According to the Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence is "information of probative value that is stored or transmitted in binary form". Thus any useful information stored or transferred in digital mode is an evidence regardless of the devices or interfaces used to store or transfer it. Therefore, smart phones are a promising site for collecting such evidence.

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". It is a flawed definition as it overlooks all possible sources for collecting digital evidence other than computers. Even the Information Technology Act 2000 (No. 21 of 2000) is not modernized to comprise information about mobile phone evidence

3.2 Principles of Electronic Evidence

United Kingdom's Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence, proposed four principles to be followed while dealing with Computer-Based Electronic Evidences [11]:

- 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 [11]. The ACPO guide also recognized that not all electronic evidence can fall into the scope of its guide and gave an example of smart phone evidence as evidence that might not follow the guide. It is also mentioned in ACPO's guide that an evidence collected without following the guide can be considered as a viable evidence.

However, Principle 1 of the ACPO guide can not be complied with when it comes to smart phone forensics. This is because smart phone storage is continually changing and that may happen automatically without interference from the mobile user. 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 [8]. According to Principle 2, the specialist must be skilled enough to understand the internals of both hardware and software of the specific smart phone device they are dealing with and be proficient with the tools used to attain 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 [8]. Coming to Principle 3, 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 [12]:

- 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 concerning to the seizure, access, storage or transfer of digital evidence must be fully documented, conserved and accessible for evaluation. 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 2 cannot 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 [10]. Hence, when using such tools for extracting information, the phone's memory may get modified unknowingly.

3.3 Mobile Phone Evidence Guides

There are a number of guides available, that concisely state potential evidence on a smart phone device. In this section, some of these guides are highlighted and their pitfalls are described.

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 [13].The details provided in these guides are not sufficient in describing an effective forensic approach for evaluating smart phones. These guides are not up to date and demand some serious modifications and extensions. Both guides though mention that mobile phones might have some potential evidence on them. The degree of the coverage is little and does not deal with 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 [12]:

- 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 [13]: Appointment calendars/information., password, caller identification information, phone book, electronic serial number, text messages, e-mail, voice mail, memos, and web browsers.

The guide overlooked the possibilities that external storage device may be attached to a smart phone.

Both the guides fail to point out that smart phones may have electronic documents, handwriting information, or location information on them. The guides do not any significance of phone based applications such as Symbian, Mobile Linux and Windows Mobile applications. Both, Symbian and Windows Mobile based phones were found to execute malicious code such as Trojans and viruses especially ones transferred via Bluetooth technology. Non malicious applications on smart phones might be used to carry out criminal actions or can have log files or useful data and thus they could also be considered as evidence or source of evidence. Thus, every phone application and content associated to it should be regarded as a probable evidence including the Bluetooth logs, Infrared (IrDA) logs , Wi-Max and Wi-Fi communications logs 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 [10].

The United Kingdom's Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence lists the following instructions (CCIPS, 2002) to be followed while handling mobile phones for evaluation processes:

- 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.

The on/off rules here initially conflict with the USSS guide. Here again the guide is not up to date for it considers only SMSs, voicemail and address book/call history details as potential source of evidence from a smart phone device. N flow chart is provided for seizure process of a smart phone.

4. PROPOSED SMARTPHONE FORENSIC MODEL: Smartphone Forensic Investigation Process Model

Many digital forensic models have already been proposed by now. However the most appropriate one has not been figured out yet. The varying frameworks developed are such that they work well with one particular type of investigation. But none of them emphasize on the specific information flow associated with the forensic investigation of Windows mobile devices.

The Windows mobile device forensic process model has been developed in an attempt to overcome the major limitations of the existing digital forensic models. It helps forensic practitioners and law enforcement officials in the investigation of crimes emphasising a systematic and methodical approach for digital forensic investigation keeping in mind that the standard practices and techniques in the physical and digital investigation world are incorporated, wherever appropriate.

The proposed model consists of twelve stages, which are explained in the subsequent sections.

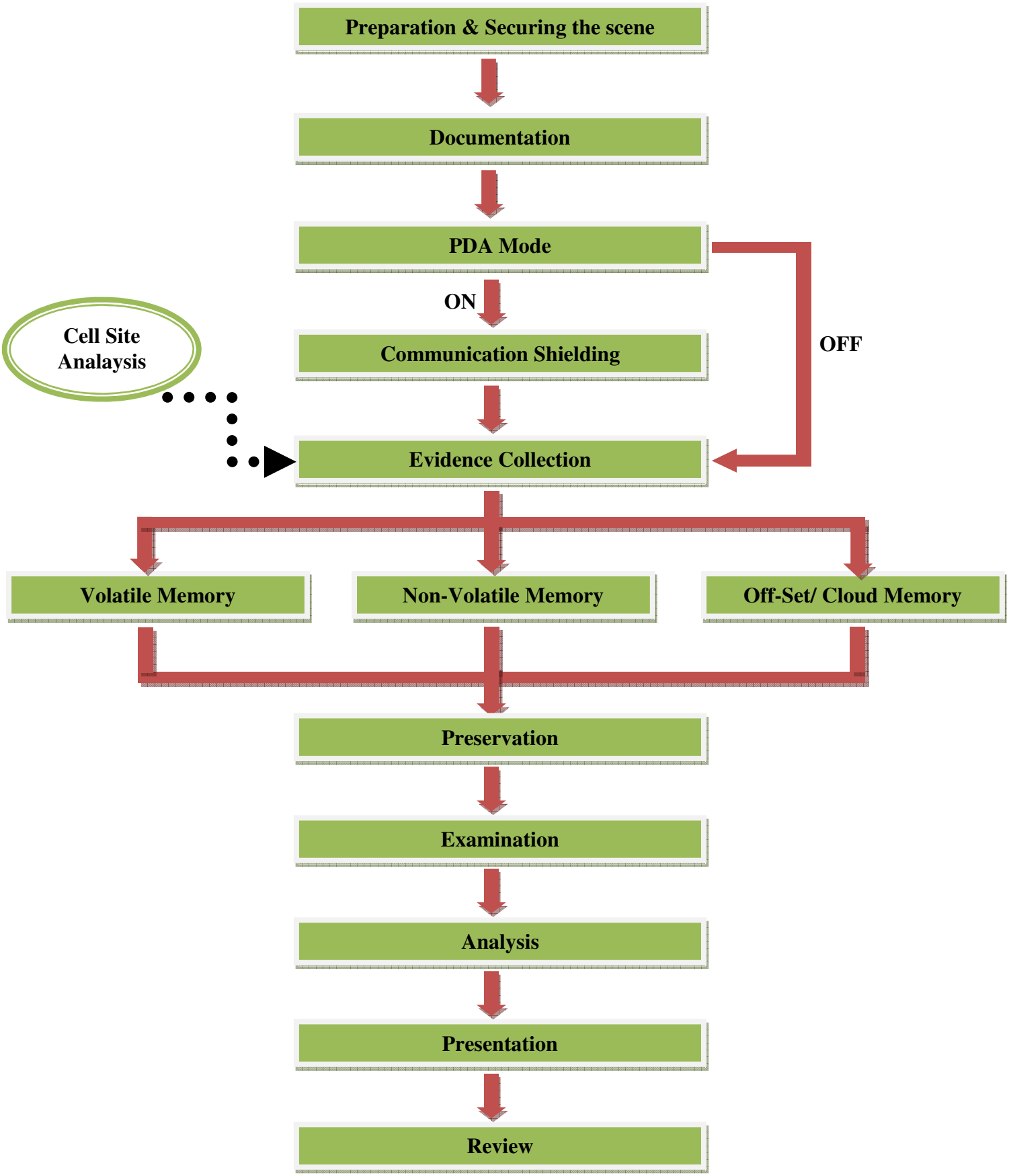

Figure 4: SFIPM

4.1 Phase One - Preparation

In order to enhance the quality of evidence and minimizes the risks associated with an investigation the preparation phase is planned out. This phase is associated with getting an initial understanding of the nature of the crime and activities. Being conducted prior to the occurrence of actual investigation, this phase involves preparation of the tools required for standard portable electronic device investigations, accumulating materials for packing evidence sources, building an appropriate team assigning roles to each personnel which may include case supervisor, crime scene sketch preparer, evidence recorder and so on, etc.

A critical assessment of the circumstances relating to the crime is carried out taking in consideration the knowledge of various mobile devices, accessories, features, specific issues etc. One more issue concerned with investigations involving Windows mobile devices is that the power runs out before evidence collection is over. So a toolkit consisting of standard power supplies, cables and cradles must be maintained properly.

A systematic strategy for investigation should be undertaken, keeping in mind the incident's nature and other technical, legal and business factors. While investigation the various legal constraints and jurisdictional as well as organizational restrictions should be ensured. Search warrants, support from the management, privacy rights of suspects, required authorizations and several other issues should not be overlooked during the process. A notification to all the concerned parties indicating the forensic investigation is also issued. Training, knowledge and experience of personnel are undoubtedly the prime contributors here.

4.2 Phase Two - Securing the Scene

Preventing the contamination and corruption of evidences and security of the crime scene from unauthorized access are the prime concerns of this stage. This is done protecting the integrity of all evidences and by maintenance of a formal protocol for ensuring systematic and secure custody at the crime spot. The evidences may get destroyed or destructed when the number of people at the crime scene increases. So Investigators are responsible for the control of the scene by defining the boundaries of the crime and controlling the gathered crowd over there. At the same time, safety of all the people at the scene must also be ensured.

It should be avoided to determine the contents in the devices and external storage devices at this stage. The devices must be left in their existing state until a proper assessment is made. If the device is on, it is better to leave it on. Similarly, if the device is off, never turn it on. No electronic device should be allowed to touch or tampered with.

4.3 Phase Three - Documenting the Scene

In order to maintain a proper chain of custody and circumstances surrounding the incident, documentation being a continuous activity is required in all stages. Things like the existing state on mobile phone when just spotted after the crime should be documented. A record of all visible data must which would help in recreating the crime scene any time during the investigation or say during a testimony in the court must be maintained. Photographs, sketches and crime-scene mapping all are merged together into a single documentation. The photographs may include device components such as power adaptors, cables, cradles and other accessories as already discussed earlier. It is necessary to keep a log of those who were present on the scene, those who reported afterwards, and those who left etc., along with the summary of their activities while they were at the scene. Classification of people into separate groups like victims, suspects, bystanders, witnesses and other assisting personnel etc. is carried out. Their location at the time of entry is recorded and documented.

4.4 Phase Four - PDA Mode

It is always advised that never to change the state of device it is working in. This phase decides the first course of action when device in hand depending upon the working of the device.

i) Active Mode: When the device is running/working, it is in Active mode or On mode. We would first need to shield it from external network and further communication without changing its mode so that the potential vulnerable volatile evidences remain intact. For this purpose device is first moved to Communication Shielding phase before working further.

ii) Inactive Mode: When the device is switched off, it is in Inactive or Off mode. Since we want to keep the evidences intact, it is not advised to turn the device on because this may lead to overriding of old data with new data. Thus we can continue with phase six and can skip communication shielding.

4.5 Phase Five – Communication Shielding

Occurring prior to the phase of evidence collection, Communication Shielding emphasizes to block the further communication options on the devices. This is done to ensure that no overwriting of the existing information on the devices is done. Even if the device appears to be in off state, some communication features like wireless or Bluetooth may be enabled.
The possibilities of overwriting and hence corruption of evidences may persist which should be avoided. Similarly, when the device is in the cradle connected to a computer and synchronization mechanisms using ActiveSync are enabled, remove any USB or serial cable, which connects it to the computer. The best option after seizing a device is to isolate it by disabling all its communication capabilities.

4.6 Phase Six – Volatile Evidence Collection

Since majority of the evidences involving mobile devices are volatile in nature, their timely collection and management is required. Volatile evidences are again prone to destruction as the device state and memory contents may change.

Depending upon the nature of evidences and the particular situation, evidences are either collected on the spot at the crime scene or they may be analyzed at the forensic laboratory afterwards. This decision may also depend upon the current power state. There may be a case of information loss if the device is running out of battery power. Hence, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. The device can also be switched off to preserve battery life and the contents of the memory. Alternatively, the contents of the memory can be imaged using appropriate commercial foreign tools like Paraben PDA Seizure which is used for memory acquisition. Several other open source forensic tools are also available which may be combined together to obtain better results.

4.7 Phase Seven – Non-volatile Evidence Collection

At this stage evidences are extracted from external storage devices like MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks etc. Along with this, evidences from computers and systems which are synchronized with these devices are also collected. Evidences of non-electric nature like written passwords, hardware and software manuals and related documents, computer printouts etc. are also looked for. Hashing and write protection of evidences is done to ensure their integrity and authenticity. Again forensic tools must be used in order to ensure the admissibility of evidences in the court of law. If the device has integrated phone features, the acquisition of sim card information takes place at this stage.

4.8 Phase Eight -- Off-Set

Until now there has been no bifurcation for the offset storage of data but the latest advancement in the field of cloud computing and other offset storage technologies has led to serious consideration of this phase for the search of potential evidence.

Smartphones are now equipped with cloud computing advantage to store their personal data online to cross mobile storage limits and access that data from anywhere anytime from any device. This could rise a possibility to hide the criminal evidence online which is not easy to track from device easily. Special consideration needs to be given to see what online data transactions have been made to have a track of activities done.

4.9 Phase Nine -- Cell Site Analysis

Cell site analysis is the science of being able to pinpoint a specific position, or positions where a mobile phone was or is. If a call is made from a mobile phone or a call is received from another phone to the mobile phone in question, or if an SMS is either sent or received then there will be records of this particular event.

Cell Site Analysis is associated with the science of locating the geographical area of the phone whenever calls are made, SMS or downloads are made or received, either in real time or historically. Such services are generally used by law enforcement agencies with the purpose of ensuring that a suspect was indeed present at on the spot and during the time when the crime was being held. The information provided is generally used for evidential purposes and is supported in courts by the expert witnesses. Using data from the networks and the skills of the network engineers, mobile phone signal strength readings are taken from various locations around the site in question to narrow down exactly where a mobile phone is being used.

4.10 Phase Ten – Preservation

To ensure the safety of evidences gathered their packaging, transportation and storage is carried out in this phase. Identification and their labeling are done before packaging. Plastic bags cause static electricity and hence may damage the evidences. Therefore, anti-static packaging envelopes are used for sealing the evidences like devices and other accessories.

Shocks, excessive pressures, humidity, temperature etc. may damage them during their transportation to the forensic workshop from the crime scene. Hence adequate precautions are necessary. Afterwards the device can be moved to a secure location where a proper chain of custody can be maintained and examination and processing of evidence can be started. Even after a safe transportation to the final destination, the packaged evidences may be prone to electromagnetic radiations, dust, heat and moisture. Unauthorized people should not have access to the storage area. National Institute of Standards and Technology guideline highlights the need of proper transportation and storage procedures, for maintaining a proper chain of custody. Proper documentation is done to avoid their altering and destruction.

4.11 Phase Eleven – Examination

To resolve and sort out the case, critical examination of the evidences collected and their analysis is carried out by the forensic specialists. Data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during this phase. Personal organizer information data like address book, appointments, calendar, scheduler etc, text messages, voice messages, documents and emails are some of the common sources of evidence, which are to be examined in detail. Finding evidence for system tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed. Detecting and recovering hidden or obscured information is a major tedious task involved.

Significance of evidences is analyzed keeping in mind their originality is maintained. Appropriate number of evidence back-ups must be created before proceeding to examination. Huge volumes of data collected during the volatile and non-volatile collection phases are filtered and split into manageable chunks and form for future analysis. Data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during this phase. A critical search and examination for decoding passwords and finding unusual hidden files or directories, file extension and signature mismatches etc. is carried out. The expertise of the investigator and capabilities of forensic tools used by the examiner also plays a major contribution for the efficient examination of evidences. When the evidence is checked-out for examination and checked-in, the date, time, name of investigator and other details must be documented. It is required to prove that the evidence has not been altered after being possessed

by the forensic specialist and hence hashing techniques like md5 must be used for mathematical authentication of data.

4.12 Phase Twelve – Analysis

Identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions etc. are some of the activities to be performed at this stage. This stage constitutes the technical review of the investigators on the basis of the results of the previous examination stage of the evidence. The analysis of whole situation at the crime scene should be such that the chain of evidences and timeline of events is consistent. Additional steps in the extraction and analysis process are analyzed and properly documented. Using a combination of tools for analysis will yield better results. The National Institute of Justice (2004) guidelines recommend timeframe analysis, hidden data analysis, application analysis and file analysis of the extracted data.

4.13 Phase Thirteen - Presentation

After the whole analysis of the results presentation of results to the wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management etc. is done. This actually depends on the nature of the crime. The findings must be presented in a court of law, if it is a police investigation or before appropriate corporate management, if it is an internal company investigation. Allegations regarding the crime are discarded or confirmed during this stage. The results of examination and analysis are reviewed in their entirety to get a complete picture. This is because the individual results of each of the previous phases may not be sufficient to arrive at a proper conclusion about the crime.

A report consisting of a detailed summary of the various events that took place during the crime and the complete description of the steps in the process of investigation and the conclusions reached is documented and provided. Along with the report, supporting materials like copies of digital evidence, devices spotted at the crime scene, a chain of custody documents, printouts and photographs of various items of evidence etc. should also be submitted. The complex terms involved in various stages of investigation process and the expertise and knowledge of the forensic examiner, the methodology adopted, tools and techniques used etc. are all likely to be challenged before a jury and needs to be explained in layman's terminology.

4.14 Phase Fourteen - Review

A complete review of all the steps during the investigation and identification of the areas of improvement are included in this final Review stage of the Windows Mobile Forensic Process Model. Results and their interpretations may be used in future for further refining the gathering, examination and analysis of evidence in future investigations. In many cases, much iteration of examination and analysis phases are required to get the total picture of an incident or crime. Better policies and procedures are established in place in future by means of this information.

Smartphone Forensic Investigation Process Model	**NIJ Law Enforcement Model**	**DFRWS Model**	**Abstract Digital Forensic Model**	**IDIP Model**	**Systematic Digital Forensic Investigation Model**
Preparation			✓	✓	✓
Securing the scene		✓		✓	✓
Survey and Recognition		✓	✓	✓	✓
Documenting the scene				✓	✓
Mode Selection/ Shielding					

Volatile Evidence Collection					✓
Non-volatile Evidence Collection	✓	✓	✓	✓	✓
Off-Set/ Online Storage					
Cell Site Analysis					
Preservation		✓	✓	✓	✓
Examination	✓	✓	✓	✓	✓
Analysis	✓	✓	✓		✓
Presentation	✓	✓	✓	✓	✓
Review				✓	✓

Table 2: Comparison of major forensic models with Smartphone Forensic Investigation process model

As it is clear from the above comparison table that not only our model is accommodating all the necessary steps but it is also including needed processes to be added to walk with the advancement in technology and look for the more efficient evidence sources. It facilitates mode selection/shielding, off-set/online storage and cell site analysis which were otherwise not supported in the rest of the models making it more effective and versatile for evidence management.

5. FUTURE CHALLENGES IN MOBILE FORENSICS

The mobile industry is moving with such a fast pace, it's often hard to keep up with it. There is a large number of future trends going to be seen with Smartphones around us. With every major mobile phone release, users are treated to an ever-expanding list of advanced features. Some are more useful than others, but they represent an industry that is always on the move.

We tried to roundup some of the best. All of these developments may have an impact on mobile device forensics.

5.1 Processor optimization

Mobile phones today are easily available with a processor speeds ranging from 300 Mhz to 600 Mhz, and even to latest Smartphones providing upto 1 to 1.3 Ghz.

Ed Hansberry stated in his article ' The Value Of Multi-Core Processors On Phones ' that Smartphones can take the benefits of symmetric multiprocessing (SMP) as well. The reason Apple has given for not allowing third party multitasking is power consumption.

Qualcomm has announced (2011) their multi-core Snapdragon line of processors, but they aren't the only one in the mobile SMP game. Most Nokia Smartphones, the Palm Pre, Motorola Droid and hundreds of other phones have an OMAP chip inside, likely an OMAP 3. Their new OMAP 4 line is based on the ARM Cortex A9 architecture.

These dual core systems do more than make things go faster, as they even overcome the challenges for mobile processors:

- Power consumption
- Digital Signal Processing
- Peripherals Integration
- Multimedia Acceleration
- Code Density

Such change in processor architecture will make an undesirable impact on Smartphone forensics.

5.2 Battery life

Power source/batter life is a major concerned these days as it was few years back before the popularity of Smartphones. Mobile phones Mobile phones typically use NiMH (nickel metal hydride), Li-ion (lithium-ion),or Li-polymer batteries. At a stage in mobile phone development these batteries were very good at their performance – look at best selling java phones like the Nokia 1100,3315,6600, Sony Ericsson T-600 etc had a battery life of almost 140 hours of standby time – nearly two weeks. But they are no so optimized enough to give this much support ot these days Smartphones simply because they require high amount of computation and continuous numerous activities running on them like GPS, wi-fi etc.

Peter Bruce, a professor of chemistry at the University of St Andrews is taking up that challenge with his "Air-Fuelled" rechargeable lithium battery. Put very simply, the Stair cell (St Andrews air cell) uses nothing more complicated than air as a reagent in a battery instead of costly chemicals. By freeing up space and exploiting one of the few elements that is free, [14] can squeeze more power into a smaller space at a reduced cost. "By using air in the cell we can get much higher energy storage up to a factor of 10.

As volatile data can be lost if the device gets turned off thus Battery life makes a huge impact on a mobile forensic investigation.

5.3 Storage memory

Smartphone's OS and applications are installed in RAM,ROM or flash memories because of the smaller OS and application as those of computers. These days latest Smartphones are available with up to 1GB of RAM to store application code and up to 64GB of internal (flash) memory for system code and user data.

Nearly every mobile phone these days also support external storage like micro SD cards varying from small storage capacity to up to large capacity of 64gb for high end Smartphones. Devices today even allow swapping in and out of external storage devices without turning off the device.
The storage medium used and the file system used by the OS to store data on it stands as a major evidence for Smartphone forensics.

5.4 Advance imaging

Smartphones are not just smart in business, they are even leading in the race of entertainment. Every Smartphone leading brand has now believed that people don't want to carry and an extra camera or camcorder to take pictures and videos thus every Smartphone releasing today is equipped with better camera technology, high pixel sensor and quality optics for advanced high quality pictures and high definition (1080p) videos.

Imaging is just not kept till photography rather advanced imagine capabilities with new mobile applications also allow to take 360 degree view of a place and make a whole map, guide, blue print of the place which can even be used for criminal offense. Thus advance imaging also stands as a source of evidence in mobile forensics and require high end image steganalysis.

5.5 Cloud computing

cloud computing is just not limited to computers in fact Smartphone leaders are trying hard to incorporate cloud with Smartphones which is going to revolutionaries the flexibility and mobile computing abilities of Smartphones.

Cloud computing rips off all the barriers which were there on the computational power of Smartphones by flexibility of the devices getting their work done remotely without having the suite installed on the device itself. It will also remove all the brand-based constraints which would be a

firm benefit with cloud implementation to any device and any application. Its de-centralized storing of documents, photographs and other data also enable users to work seamlessly with colleagues and even share devices without loss of data.

But we can deny that cloud computing in Smartphones also increases the risk of criminal activities being carried out in a more planned and larger scale because of seamless sharing and group working of people which could lead to large terrorist activities too.

5.6 4G and beyond

After 3G, the arrival of 4G is threatening to occur immediately and with it comes a new array of functionality along with higher specification hardware and improved network infrastructure which is going to enhance the speed of our mobile lives. It also going to provide fast and stable data connection.

This rapid change in technology and its extension is a big hurdle in Smartphone forensics. With new technology comes the requirement of newer way of Smartphone forensics.

6. CONCLUSION

Motivated by the rapid increase in mobile frauds and cyber crimes, this research work took tried to put forward the need and way of Smartphone forensics. This paper starts with the discussion on the increasing need of smartphone forensic then how is it different from computer or other digital forensics and then moving on to potential evidences and strategies defined earlier.
The proposed Smartphone Forensic Investigation Process Model (SPFIPM) benefits as follows:
• Serve as benchmark and reference points for investigating Smartphones for criminal cases.

• Provide a generalized solution to the rapidly changing and highly vulnerable digital technological scenario.

7. REFERENCES

1. Nielsen. “Mobile Texting Status.” Internet: http://mashable.com/2010/10/14/nielsen-texting-stats/, Oct. 14, 2010 [Jan. 13, 2012]

2. D. Paul. “the year of mobile customers.” Internet: http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_release_Nov07.pdf, Nov. 07, 2011 [Jan. 15, 2012]

3. FoneKey. Internet: www.FoneKey.net, 2008 [Dec. 12, 2011]

4. Ducell. Internet: www.DuCell.org, 2008 [Dec.15, 2011]

5. D, Mock. “Wireless Advances the Criminal Enterprise.” Internet: http://www.thefeaturearchives.com/topic/Technology/Wireless_Advances_the_Criminal_Enterprise.html, Jun. 18, 2008 [Jan. 17, 2012]

6. R. Ayers, W. Jansen, N. Cilleros & R. Daniellou. “Cell Phone Forensic tools: An Overview and Analysis.” Internet: http://csrc.nist.gov/publications/nistir/nistir-7250.pdf, 2007 [Jan. 21, 2012]

7. B. D. Carrier. “Risks of Live Digital Forensic Analysis.” Communications of the ACM, 49(2), 56-61.

8. W. Jansen & R. Ayers “Guidelines on Cell Phone Forensics” Internet: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf, 2006 [Feb. 03, 2012]

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

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

11. ACPO. “Good Practice Guide for Computer based Electronic Evidence.” Internet: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, 2003 [Dec. 22, 2012]

12. IOCE. “Best Practice Guidelines for Examination of Digital Evidence.” Internet: http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf, 2007 [Feb. 09, 2012]

13. NIJ. “Electronic Crime Scene Investigation: A Guide for First Responders.” Internet: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 2003 [Feb. 11, 2012]

14. U. Simon. “Batteries: The power behind the phone” Internet: http://www.independent.co.uk/life-style/gadgets-and-tech/features/batteries-the-power-behind-the-phone-1872933.html, Jan. 2010 [Feb. 18,2012]

15. A. Ankit, G. Megha, G. Saurabh & C. Gupta. “Systematic digital forensic investigation model” Vol. 5 Internet: http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf, 2011 [Jan. 15, 2012]