

# Forensic Extraction of Mobile Phone: A Challenge for Law Enforcement

## OVERVIEW: MOBILE FORENSIC

As the mobile phone become inevitable in every business process and makes the life easier. It is considered that use of mobile phone increases transparency and accountability as well as maximizes the business profit also. The versatile function of mobile phone makes it very popular in every age group. In the present scenario mobile phone become identity of person. Mobile phones the only thing that is common to every single criminal from a petty thief to a king-pin who specialises in kidnapping industrialists. The latest challenge in front of police intelligence department is to track down a mobile phone. *“If some body is calling from a land-line, it is a matter of a few seconds for us to track down the caller. But it becomes difficult when the same call is made from a mobile phone,”* said a senior official of the city police special branch. (Time of India, 23.2.08)

The city police and the criminal investigation department are now working jointly towards pinning down a criminal even if he is calling from a mobile phone. Thus mobile phone becomes ample source of evidence for the investigative purpose and acquittal. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. The forensic validity is an important issue for acquiring data from a mobile phone as admissible evidence. Information collected from mobile phones is increasingly required as evidence in criminal investigations.

As the awareness of user increases and the technological improvement in mobile phone, it contain a large amount of information related to the user's actions, determined by their communication patterns, and information such as images, video and audio recordings. Similarly, the information stored in a mobile phone becomes important in proving or disproving theories and allegations. (Pramod Mahajan murder case)

The Indian legislation considered a mobile phone in the same manner as a computer, or any other electronic device. The seized device must be shown that the device is functioning correctly, before information produced by such a device can be admitted as evidence. The procedures used to obtain the information must be documented properly and do not adversely affect the validity of the information.

Hence, the methods of extracting information from a mobile phone effect directly on originality of the information or whether that information will be admissible as evidence. If a certain method indicates to alter data on the phone, integrity of that data may be questioned, and even shown to be inaccurate. The desired situation would occur when a method can be proven to acquire data without making any changes to the phone's memory; information acquired using such a method will be admissible as evidence.

## METHOD OF STUDY

The beginning of effort to this study was the literature review in order to understand the concept and enhance the knowledge towards the topic. The earlier academic research in the area was documented. In addition, a brief overview of the methods commonly used to acquire data from mobile phones, and the procedures, which should be followed when forensically analysing a mobile phone, was produced. The Indian legislation system was analysed to determine how the law applies to information obtained from a mobile phone. There are only a few sections which specifically relate to the admissibility of electronic information as evidence; Sections 65 A and 65 B the Evidence Act 1995 (Ammended) relates to proving that evidence produced by a device is correct. Besides Indian IT Act 2000 widely accept the legacy of electronic record.

Well known from its initial, that multiple issues arise regarding the integrity and reliability of Mobile devices during forensic testing. These can be securing the data, ensuring that all possible data is recovered and other variables that could compromise potential evidence. The following procedural guidelines were established and used during the forensic analysis of the mobile devices. The method

was specifically designed to meet the objective of the study. Although concept of study was clear but the challenges towards law enforcement agencies were also discussed.

## **Result**

The information collected was quite interesting, though for privacy reasons, recovered information could not be disclosed. The report generated by the tools was useful for reexamining because individual areas of interest could be searched easily. Also the MD5 and SHA1 hash was simple to locate (due to it being displayed in a report) and did not require extensive effort to discover.

## **Challenges to law enforcement**

As discussed previously mobile evidence is considered a very new, so it is possible that lack of knowledge towards the technology by the Police, the Lawyers and the Judges effect negative consequence on the judicial decisions.

The important aspects for which Mobile evidence is being presently used are

- Numbers to which calls have been made from a given mobile with date and time
- Numbers from which the calls have been received in a given mobile with date and time
- Phone book of devices.
- Details of recent SMS messages received
- Details of SMS templates
- Ring tones and Games stored in the instrument
- Pictures and video clips stored in the mobile either on the SIM card or a flash memory card.

All of these some are available from the service provider while some are available from the device. It is considered that data available from service provider is more reliable then device due to its short memory and processor.

The challenges arises on the integrity of the data, If the data provided by provider's equivalent the data of recently called and received numbers, it implies that SIM card data is original. Consequently the data from the SIM card taken as only representative confirmation and has to be appropriately certified to be of any use in a court of law.

If the data on the SIM card is extracted from the Mobile after the mobile has been in the custody of the Police for some time, it is possible for the defense to take a stand that the data has been manipulated.

On the other hand the data at the service provider's level cannot be manipulated except with the connivance of the service provider or hacking into their system. Again here the data as found visible on the computers of the service provider can be taken as prima facie evidence but if it has to be relied upon, there has to be a corroborative certification that the data is apparently not altered.

Since mobile conversations are not presently recorded by the service provider and they are not normally available for any evidence. If the conversation is hacked and recorded, then it will be a case of illegal tapping and the quality of the evidence needs to be evaluated by other parameters including voice recognition.

The phone book details only provide information about the persons whom the mobile owner has been in contact and nothing more.

A few of the incoming SMS messages are normally stored on the mobile and along with time data corroborated with the service provider's information, may be evidence of an incoming message. Templates may indicate the likely outgoing information and if it contains any spam or obscene message, may indicate the intention of the mobile user and nothing more.

Copyright violations relevant during the overview of handset in concern to ringtone and video game.

Details of pictures and video clippings on an accompanying memory card indicates the intentions of the mobile user and if they can be matched with any outgoing data packets, may be used as evidence for the likely outgoing message. These can be of use in case of any obscene pictures being transmitted from the mobile.

## **Conclusion**

Lastly it can be concluded that the whole study got its shape into its partial success. During investigation deleted information from devices was not recovered. The limitation of tool can be observed very easily due to its limited application while the major problem of accessing different type of mobile devices formed the study very limited.

But the clear and defined step of testing procedure ensures the integrity of data as well as quality of investigation. Further lack of researches into this area tied the whole study and discoveries needed to strengthen the area. The bigger challenge to the law enforcement agencies was to fail to comply with validated testing procedures can face serious consequences in regards to ensuring the integrity of their findings. Besides, lack of technical knowledge to the investigating and judicial people create greater problem in decision. Adding to more on this uniform set of testing procedure and standard method is the demand of future. As this area is quite immature, the efforts made currently are not fully guaranteed.