Mobile Forensics: overview of digital forensic, computer forensics vs. mobile forensics and tools

Shubhangi Daware,
Sandhya Dahake
MCA, G. H. Raisoni Institute of Information Technology. Nagpur

V. M. Thakare
Head of the Department P. G. Dept of Computer of Science & Eng. Technology S.G.B. Amravati University, Amravati

ABSTRACT
Now a days the growth of advanced life the mobiles and computers are very necessary components to be considered for the progress. The continued growth of the mobile device market, the possibility of their use in criminal activity will only continue to increase. The mobile device market provides many manufactures and models causing a strong diversity. Due to such features and facilities , people will more depend on application such as SMS, MMS, Internet Access, Online Transactions etc. There are many tools and techniques available to identify and investigate the crimes done with the help of mobiles or computers. So, it becomes difficult for a professional investigator to choose the proper forensics tools for seizing internal data from mobile devices. Such mobile devices also provides a good source of evidence for forensic investigators to prove or disprove the commitment of crimes of victims. Through this paper, we will give an overview of digital forensic process and tools and also the comparison between computer and mobile forensics. Each popular digital forensic tool and offer an inside view for investigators to choose their free sources or commercial tools. Also we have focused on the area and applications of digital forensics.

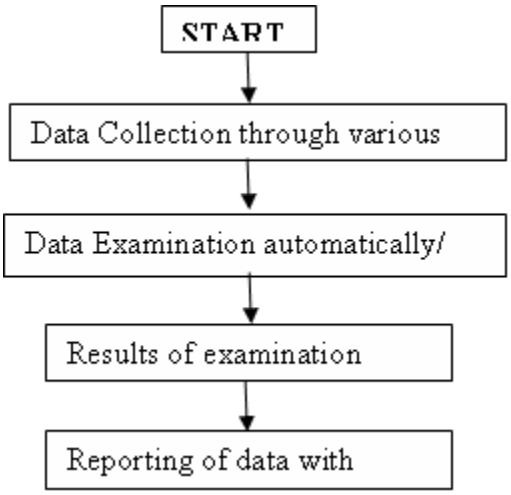
Keywords
Forensic, Digital, Evidence,Investigation, Process New Start Material

1. INTRODUCTION
Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Digital forensic is a collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence. It is also a methodology for computer investigation and analysis techniques in the interest of determining potential legal evidence. It is a process of extracting ***evidence*** from computers or other digital devices Usually involves extracting the contents of files and interpreting their meanings.

Digital forensics - "computer forensics" in older terminology - is the discovery, recovery, and investigation of digital information. The term "digital forensics" is usually used in connection with the investigation of a crime. But it also applies to recovery of an accidentally deleted file, or a forgotten password. Digital forensic techniques involve the application of science to the identification, collection, examination, and analysis of data in ways that preserve the integrity of the information and maintain a strict chain of custody for the data. Organizations have the means to collect growing amounts of data from many sources. Data is stored or transferred by standard IT systems, networking equipment, computing peripherals, personal digital assistants (PDAs), consumer electronic devices, and various types of media. When information security incidents occur, organizations that have established a capability to apply digital forensic techniques can examine and analyze the data that they have collected, and determine if their systems and networks may have sustained any damage and if sensitive data may have been compromised. Digital forensic techniques can be used for many purposes, such as supporting the investigation of crimes and violations of internal policies, analyses of security incidents, reviews of operational problems, and recovery from accidental system damage.

2. THE BASIC FORENSIC PROCESS
A four-step process for applying digital forensic techniques in a consistent manner:

- **Collection:** Data is identified, labeled, recorded and acquired from all of the possible sources of relevant data, using procedures that preserve the integrity of the data. Data should be collected in a timely manner to avoid the loss of dynamic data, such as a list of current network connections, and the data collected in cell phones, PDAs, and other battery-powered devices.
- **Examination:** The data that is collected should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the specific situation, while preserving the integrity of the data.
- **Analysis:** The results of the examination should be analyzed, using well-documented methods and techniques, to derive useful information that addresses the questions that were the impetus for the collection and examination.
- **Reporting:** The results of the analysis should be reported. Items to be reported may include: a description of the actions employed; an explanation of how tools and procedures were selected; a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.



Flow of Digital Forensic Process

The digital forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation. Mobile phones are commonplace in today's society, used by many individuals for both personal and professional purposes. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. When a cell phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the phone be handled? How should valuable or potentially relevant data contained on the device be examined? The key to answering these questions is an understanding of the hardware and software characteristics of cell phones.

Different types of digital cellular networks abound that follow distinct incompatible sets of standards. The two most dominant types of digital cellular networks are known as Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. Other common cellular networks include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). IDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols. A digital version of the original analog standard for cellular telephone phone service, called Digital Advanced Mobile Phone Service (D-AMPS), also exist.

Mobile phones work with certain subsets of the network types mentioned, typically those associated with the service provider providing the phone and from whom a service agreement was arranged. For example, a service provider or network operator for a GSM network that has some older TDMA network segments in operation might supply a phone that has GSM voice and data capabilities, and TDMA capabilities. Such a phone would not be compatible with CDMA networks. Mobile phones can also be acquired without service from a manufacturer, vendor, or other source, and have their service set up separately with a service provider or network operator, provided that the phone is compatible with the network. When in operation, mobile phones may contact compatible networks operated for or by another service provider, and gain service. To administer the cellular network system, provide subscribed services, and accurately bill or debit subscriber accounts, data about the service contract and associated service activities are captured and maintained by the network system.

The general hardware characteristics of basic, advanced, and smart phone models, which underscore this diversity.

Table 1: Hardware Characterization

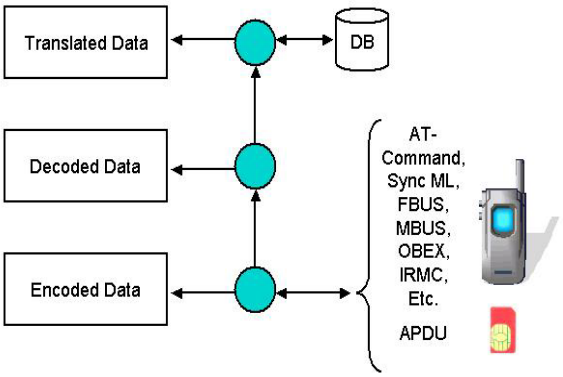
	Basic	Advanced	Smart
Processor	Limited Speed	Improved Speed	Superior Speed
Memory	Limited Capacity	Improved Capacity	Superior Capacity, Built-in Hard Drive Possibility
Display	Grayscale	Color	Large size, 16-bit Color (65,536 colors) or Higher
Card Slots	None	MiniSD or MMC mobile	MiniSDIO or MMCmobile
Camera	None	Still	Still, Video
Text Input	Numeric Keypad	Numeric Keypad, Soft Keyboard	Touch Screen, Handwriting Recognition, Built-in QWERTY-style Keyboard
Cell Interface	Voice and Limited Data	Voice and High Speed Data	Voice and Very High Speed Data
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi
Battery	Fixed, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion

The situation with forensic software tools for cell phones is considerably different from personal computers. While personal computers are designed as general-purpose systems, cell phones are designed more as special-purpose appliances that perform a set of predefined tasks. Cellular phone manufacturers also tend to rely on assorted proprietary operating systems rather than the more standardized approach found in personal computers. Because of this, the variety of toolkits for mobile devices is diverse and the range of devices over which they operate is typically narrowed to distinct platforms for a manufacturer's product line, an operating system family, or a type of hardware architecture. Short product release cycles are the norm for cellular phones, requiring tool manufacturers to update their tools continually to keep coverage current. The task is formidable and tool manufacturers' support for newer models often lags significantly. Some have argued that the current state is likely to continue, keeping the cost of examination significantly higher than if a few standard operating systems prevailed.

Forensic tools acquire data from a device in one of two ways: physical acquisition or logical acquisition. Physical

acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip), while logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e., a logical view), versus memory as seen in raw form by the processor and other related hardware components (i.e., a physical view).

Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present (e.g., in unallocated memory or file system space) to be examined, which otherwise would go unaccounted. Extracted device images need to be parsed, decoded, and translated to uncover the data present. The work is tedious and time consuming to perform manually. Physical device images can be imported into a tool to automate examination and reporting, however, only a few tools tailored for obtaining cell phone images are currently available. A logical acquisition, though more limited than a physical acquisition, has the advantage that the system data structures are normally easier for a tool to extract and provide a more natural organization to understand and use during examination. If possible, doing both types of acquisition is preferable – a physical acquisition before a logical acquisition.



Comparison digital/computer forensics with mobile forensics

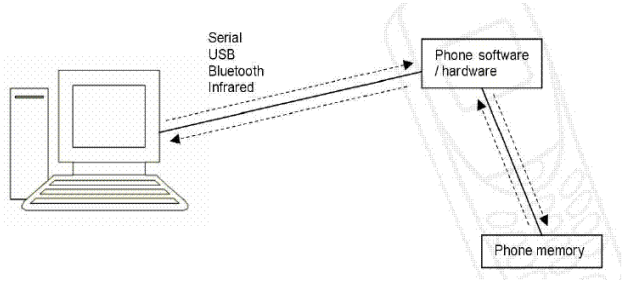
1. Reproducibility of evidence in the case of dead forensic analysis- One of the key differences between traditional computer forensics and mobile phone forensics is the reproducibility of evidence in the case of dead forensic analysis. This is due to the nature of mobile phone devices being constantly active and updating information on their memory.

2. Connectivity options and their impact on dead and live forensic analysis - 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.

3. Operating Systems (OS) and File Systems (FS) 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. 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. Mobile phone operating systems are generally closed source with the exception of Linux based mobile phones. This makes developing forensics tools and testing them difficult task. 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. One of the drawbacks currently facing mobile OS and FS forensic development is the extremely short OS release cycles.

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.

5. ***Forensic Tools and Toolkits Available*** - 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.



3. CONCLUSION

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.

4. APPLICATIONS

[1] Digital forensic is applicable in the future Enterprise Resource Planning Systems.

[2] Recent development in digital image processing

[3] Accuracy enhancement in environment sound recognition using ZC features and MPEG-7 with modified K-NN classifier feature

[4] Digital forensic in VoIP Networks

[5] Development and Application of Digital Forensic Logging System for Data from a Keyboard and Camera

[6] An Analysis of the Digital Forensic Examination of Mobile Phones

[7] References

[8] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[9] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[10] S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[11] K. Elissa, "Title of paper if known," unpublished.

[12] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[13] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[14] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[15] Aljazeera (2005). Phone Dealers in al-Hariri Probe Net, URL,

[16] http://www.idc.com/getdoc.jsp?containerId=prUS213 03808, 6. FoneKey (2008). URL, www.FoneKey.net, 7. Ducell (2008). URL, www.DuCell.org, 8. Mock,

[17] Computer Forensic Tool Testing Program, Computer Imaging Specification, Version 3.1.6, National Institute of Standards and Technology. Available at: www.cftt.nist.gov

[18] Eckert, W. G., Introduction to Forensic Sciences, 1997, CRC Press.

[19] Federal Rules of Evidence, Article VII. Opinion and Expert Testimony, Rule 702 & Rule 703. Available at: www.house.gov/judiciary/evid00.pdf

[20] Foster, K., R Huber, Judging Science: Scientific Knowledge and the Federal Courts, 1997, MIT Press.

[21] Koehler, J. J., A. Chia, S. Lindsey, , "The Random Match Probability in DNA evidence: Irrelevant or Prejudicial," Jurimetrics Journal, 1995, Winter, pp. 201-219.

[22] Pollack J., US District Court, PA: U.S. v Plaza, Acosta (Cr. No. 98-362-10, 11,12), "Strengthening the Criteria for Admissibility of Fingerprint Evidence," Judicial Opinion. Available at: www.paed.uscourts.gov/documents/opinions/02D004 6P.htm