MOBILE DEVICE FORENSICS

P Sree Gayathri

M.Tech (CSE), V.R Siddhartha Engineering College

***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. Finally, highlights some of the Mobile Forensics Challenges.

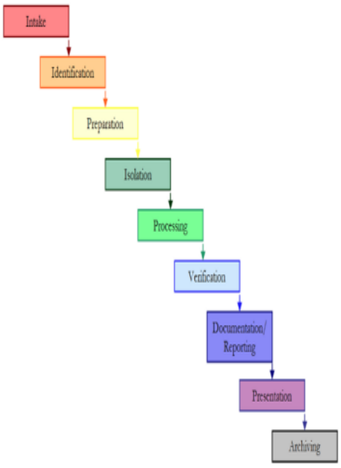
I. Introduction

Over the past several years, digital forensic examiners have seen a remarkable increase in requests to examine data from cellular phones and other mobile devices. The examination and extraction of data from these devices presents numerous unique challenges for forensic examiners. With smart phones and tablets representing an increasing proportion of mobile devices submitted for examination, the number unique challenges continue to grow.

Some of those challenges include the following not only are there a large variety of mobile devices available commercially, those devices use a variety of proprietary operating systems, embedded file systems, applications, services, and peripherals. Each of these unique devices may be supported to different extents by the available forensic software tools, or may not be supported at all. There is also generally significant lag time before newer smart phone devices are supported sufficiently by mobile forensic tools. The types of data contained within mobile devices and the way they are being used are constantly evolving. With the popularity of smart phones, it is no longer sufficient to document only the phonebook, call history, text messages, photos, calendar entries, notes and media storage areas because these devices are fully functioning minicomputer sand potentially contain much more relevant data. The data from an ever-growing number of installed applications can contain a wealth of relevant information that may not be automatically parsed by available forensic software solutions. Traditional digital forensic skills are becoming more and more necessary for mobile device examinations.

Cellular phones and other mobile devices are designed to communicate with cellular and other networks via radio, Bluetooth, infrared and wireless (Wi-Fi) networking. To best preserve the data on the phone it is necessary to isolate the phone from surrounding networks. This may not always be possible, and isolation methods can be prone to failure. Mobile devices use a variety of internal, removable and online data storage capabilities. In many cases, it is necessary to use more than one tool in order to extract and document the desired data from the mobile device and its associated data storage media. In certain cases, the tools used to process cellular phones may

The reasons for the extraction of data from cellular phones may be as varied as the techniques used to process them. Cellular phone data is often desired for intelligence purposes and the ability to process phones in the field is attractive. Because of these factors, the development of guidelines and processes for the extraction and documentation of data from mobile devices is extremely important, and those guidelines and processes must be periodically reviewed as mobile device technology continues to evolve and change. What follows is an overview of process considerations for the extraction and documentation of data from mobile devices.



II. 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

Furthermore, technologies such as “push email “and always on connections added convenience and powerful communications capabilities to mobile devices. Push email provided users with instant email notification and download capability, where when a new email 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.

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 (EWallet) 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.

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-wayhashfunction 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 bitwise copy of the entire hard disk.

After that, the acquired image is analyzed in a lab using a trusted OS and sound forensic applications. 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 (Jansen &Ayers 2006). This means that it will be impossible to attain a bitwise copy over the entire contents of a mobile phone’s memory.

Connectivity Options and Their Impact on Dead and Live Forensic Analysis

Live forensic analysis in this context refers to online analysis verses 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. Evnethough 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.

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. Another issue with mobile OS and FS when compared to computers is the states of operation. 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 lifecycle 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 2006). This short release cycle makes timely development, testing and release of forensic tools and updates that deal with the newer OS releases difficult toachieve.

Hardware

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

The hardware architecture of a typical mobile phone usually consists of a microprocessor, main board, ReadOnly 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 abattery. The OS usually resides in ROM while RAM is generally used to store other data such as user data andgeneral user modifiable settings.

The ROM may be reflashedand updated by the user of the phone bydownloading a file from a web site and executing it on a personal

tools is usually slow. The following section discusses in moredetail some of the mobile forensic tools and their features and drawbacks when compared to computer basedforensic tools.

Forensic Tools and Toolkits Available

Early mobile phones did not have the capacity to store large amounts of information so law enforcement officersdid not need to access mobile phone handsets to get information on a suspect. The focus was more on phonerecords from the telecommunications companies. Nowadays, mobile phones have large storage capacity and awide array of applications and connectivity options besides connectivity with the telecommunications provider.

This inherent difference between computer forensics and mobile phone forensics effects how data acquired frommobile phones is perceived.

To make this data trustable, independent evaluation of mobile forensic tools has tobecome an integral part of their development.

The only currently available tools evaluation document for mobilephone forensics is published by the National Institute of Standards and Technology (NIST) in the United States

III. MOBILE FORENSIC CHALLENGES

One of the biggest forensic challenges when it comes to the mobile platform is the fact that data can be accessed, stored, and synchronized across multiple devices. As the data is volatile and can be quickly transformed or deleted remotely, more effort is required for the preservation of this data. Mobile forensics is different from computer forensics and presents unique challenges to forensic examiners.

Law enforcement and forensic examiners often struggle to obtain digital evidence from mobile devices. The following are some of the reasons:

Hardware differences: The market is flooded with different models of mobile phones from different manufacturers. Forensic examiners may come across different types of mobile models, which differ in size, hardware, features, and operating system. Also, with a short product development cycle, new models emerge very frequently. As the mobile landscape is changing each passing day, it is critical for the examiner to adapt to all the challenges and remain updated on mobile device forensic techniques.

Mobile operating systems: Unlike personal computers where Windows has dominated the market for years, mobile devices widely use more operating systems, including Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS, and many others.

Mobile platform security features: Modern mobile platforms contain built-in security features to protect user data and privacy. These features act as a hurdle during the forensic acquisition and examination. For example, modern mobile devices come with default encryption mechanisms from the hardware layer to the software layer. The examiner might need to break through these encryption mechanisms to extract data from the devices.

Lack of resources: As mentioned earlier, with the growing number of mobile phones, the tools required by a forensic examiner would also increase. Forensic acquisition accessories, such as USB cables, batteries, and chargers for different mobile phones, have to be maintained in order to acquire those devices.

Anti-forensic techniques: Anti-forensic techniques, such as data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult.

Dynamic nature of evidence: Digital evidence may be easily altered either intentionally or unintentionally. For example, browsing an application on the phone might alter the data stored by that application on the device.

Accidental reset: Mobile phones provide features to reset everything. Resetting the device accidentally while examining may result in the loss of data.

Device alteration: The possible ways to alter devices may range from moving application data, renaming files, and modifying the manufacturer's operating system. In this case, the expertise of the suspect should be taken into account.

Pass code recovery: If the device is protected with a pass code, the forensic examiner needs to gain access to the device without damaging the data on the device.

Communication shielding: Mobile devices communicate over cellular networks, Wi-Fi networks, Bluetooth, and Infrared. As device communication might alter the device data, the possibility of further communication should be eliminated after seizing the device.

IV. CONCLUSION

With increased connectivity options and higher storage capacities and processing power, abuse of mobile phonescan becomes 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 (Long2005).

V. REFERENCES

[1] Becker, D. (2005). Toshiba Reports Battery Breakthrough, URL http://news.com.com/206110786_35649141. html?tag=nl Carrier, B. D. (2006). Risks of Live Digital Forensic Analysis. Communications of the ACM, 49(2), 5661.

[2] CCIPS. . Searching and Seizing Computers and Related Electronic Evidence Issues, URL

[3] http://www.usdoj.gov/criminal/cybercrime/searching.html.

[4] Espiner, T. (2006). Mobile Phone Forensics 'Hole' Reported, URL

[5] http://news.zdnet.co.uk/hardwe/0,1000000091,39277347,00html.IOCE. (2002).