Survey on Mobile Forensics

Ritika Lohiya
Institute of Technology
Nirma University
Ahmedabad

Priya John
Institute of Technology
Nirma University
Ahmedabad

Pooja Shah
Prof., Institute of Technology
Nirma University
Ahmedabad

ABSTRACT

With the continued growth of smart phone market, the probability of their use in criminal activities has continued to increase. Mobile phone nowadays comes with a wide variety of software application, new technologies and operating systems. Therefore it becomes complicated for a forensic investigator to examine the evidence from a mobile phone. A proper knowledge of forensic tools and their features is required to collect relevant information. This paper discusses about the mobile device characteristics, the steps for mobile forensic investigation and different tools for mobile forensics. The last section of the paper presents the experimental results of the tools Mobiledit Lite and Autopsy 3.1.2.

General Terms

Mobile Forensics, Digital Forensics, Forensic Investigation, Smart phones

Keywords

Mobile Forensics, Forensic Tools, Forensic Investigation.

1. INTRODUCTION

In essence, Forensic Science is often referred to as gathering and examining the information of an event or a crime. With the technological advancement, forensic science has evolved to a great extent. Forensic investigation processes often relay on the evidence collected by the officials and these evidences are often in the digital form. And this process of analysing the digital information for investigation is known as digital forensics. According to National Security Database (NSD), digital forensics is a branch of forensic science which deals with the retrieval and investigation of material found in digital devices.

Earlier digital forensics was often used to describe the process of forensic investigation of the crimes which are mostly related to computer. Digital forensics was used to describe the crime in which either the computer has been used as a weapon to conduct the criminal activities or computer has been the victim of the crime. But nowadays digital device is not limited to 'computer'. Today digital device includes computer, mobile phones, tablet or any electronic device. Forensic investigation process does not depend on the type of digital device used, rather the process of investigation is the same for all kind of digital devices. The investigation process mainly has three phases: data acquisition which includes acquiring the data from the device if it is in the sound condition and in damaged condition the mirror image of the device is produced which is the used for data retrieval. The next phase is analysis in which the data acquired is analysed for evidence gathering. And the last phase is preservation which includes keeping the data and the evidence collected in safe condition which further could be used for the presentation of evidence in the court of law.

Digital forensic is a discipline which includes computer forensics, mobile forensics and network forensics. The scope of this paper is to focus on 'Mobile Forensics'.

Mobile forensics is a branch of digital forensics which concerns with retrieving the data from a mobile device under forensically sound conditions. The revolution in mobile forensics is completely due to the invention of the smart phones which are equipped with the complete operating system, software applications and look and feel which make the interaction with the user easy and comfortable.

Mobile forensics consists of the methods which describes how to take evidence from the mobile phones and how to analyse them for information retrieval. It consists of analysis of SIM and the phone memory. Mobile phone are capable of storing information just like we store it on our computers and therefore recovering the deleted information from a phone is as similar as to recover it from a hard disk.

The best example of mobile phone used as a terror weapon to execute the crime is the Mumbai terrorist attack in 2008. The terrorist took the full advantage of being a part of the mobile phone generation. They connected electronically to each other as well as their controllers during every phase of their operation. This attack is not the first time where mobile phone is used, but the way it was executed is significant and revealing. In such cases there is a large amount of data that can be extracted from these devices and used as forensic evidence.

2. MOBILE DEVICE CHARACTERISTICS

Mobile phones are capable of executing multiple tasks ranging from a simple call to storing and preserving data just like a personal computer. They are mobile, compact in size, with well powered battery and are light in weight. The basic set of features include a house of microprocessor, read only memory (ROM), random access memory (RAM), microphone, speaker, digital signal processor, a number of hardware keys and interfaces and liquid crystal display (LCD). The NAND or NOR memory of the mobile device consists of the operating system while the code execution occurs in RAM.

Mobile devices consist of system level microprocessors which provide the considerable internal memory and also reduce the number of supporting chips required. Mobile phones consist of different physical characteristics such as size, memory

capacity, processor, speed etc. Also nowadays smart phones come with many facilities like Global Positioning Systems (GPS) which is used for navigation and location finding, cameras which are capable of capturing still images as well as video recording, office suite which is capable of storing files and documents just like a personal computer. Earlier mobile phones were much simpler which were basically used for simple voice and messaging communications. There were no facilities as provided by the smart phones and therefore the mobile devices with such simple look and feel were often referred to as featured mobile phones.

Below are two tables which differentiate between the featured phone and a smart phone by classifying them on the basis of the hardware and software characteristics.

Table 1. Hardware Characteristics of Mobile Device

Category	**Feature Phone**	**Smart Phone**
Processor	Speed is Limited	Speed is superior to the featured phone.
Memory	Memory is Limited	Memory is superior to that of a featured phone.
Display	Small size colour display (12 bit-18 bit)	Large size colour display (approx 24 bit)
Card Slots	None	MiniSDXC
Camera	Still	Still and Video (HD)
Text Input	Numeric Keypad	Touch Screen, Built-in QWERTY keypad
Voice Input	None	Voice Recognition (Dialing and Control)
Positioning	None	GPS receiver
Wireless	IrDA, Bluetooth	Bluetooth, WiFi and NFC

Mobile phones have a number of software applications and these applications have a set of features. The table below describes the software characteristics of the mobile devices.

Table 2: Software Characteristics of Mobile Device

Category	**Feature Phone**	**Smart Phone**
Operating System	Closed	Andriod, BlackBerry, Windows, iOS
Personal Information Management	Phonebook, Calender and Reminder List	Enhanced Phonebook, Calender and Reminder List
Applications	Games, notepad etc	Games, office suite, social media, music etc
Call	Voice	Voice and Video
Messaging	Text messaging	Full multimedia messaging
Email	Via text messaging	Via POP or IMAP server
Web	Via WAP gateway	Direct HTTP

3. MOBILE DEVICE OPERATING SYSTEM

The first thing to be investigated while examining a mobile phone as evidence is whether its Operating System is compatible with the forensic tool being used by the forensic scientist. There are two types of Operating Systems - Open Source and Proprietary.

Android OS: The Android OS is based on Linux 2.6 kernel that acts like an intermediary between the hardware and the remaining hardware stack. The Linux kernel is responsible for provision of services such as process management, memory management, Inter Process Communication, network protocol stack, drivers, and security. The framework used in Android follows object-oriented approach and allows reuse of existing System, Java and C/C++ libraries. Dalvik VM is a Java virtual machine (VM) that is designed in such a way that it utilizes limited system resources during execution. (Source: http://www.***cse****web.ucsd.edu/classes/fa10/****cse120/lectures/CSE120-lecture.pdf***)

iOS: The iOS is based on UNIX Operating Systems and derived from Mac OS X operating system. The foundation framework is responsible for providing services such as file management and network management. Using the framework and Objective C Language, applications are created and executed on the iPhone directly on the iOS itself. The core OS layer provides services such as peer to peer connectivity, security, authentication, concurrency, I/O management, supports for networking and digital signal processing. (Source: *https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iphoneostechoverview/iOSTechOverview.pdf*)

Blackberry OS: The Blackberry OS [10] is a proprietary system. It was developed for corporate professional to stay connected even while travelling. The major APIs such as memos, calendars, and Java applications access the Research in Motion (RIM) Java Virtual Machine (JVM). Its functioning is similar to Android which also relies on Java Virtual Machine. Mobile Data Service (MDS) deals with internet related tasks like push mail, instant messaging and file sharing.

Windows Phone: The Windows Phone is derived from Windows OS. The essential components of the OS such as the kernel, graphics support, networking support, file management and media file handling is managed by the core OS layer. At a lower level, the OS components of Windows Phone 8 and Windows 8 are the same. In case of sudden power failure, data recovery is possible by analyzing the Transaction- Safe FAT file. NAND and NOR are the two types of flash memory used in Windows Phone. (Source: www.cl.cam.ac.uk/~acr31/p36/WP8%20Development%20Cambridge.pdf)

Symbian OS: The Symbian OS Core is responsible for abstraction of the hardware layer. Kernel, Memory management, Event management and drivers have the same Symbian OS core. Services for communication like TCP/IP and SMS are implemented at the System Layer i.e. top of the Symbian OS core. Since object oriented design is used in Symbian OS, components or hardware can be added / removed. The basis of Symbian OS lies on agreed open standards. Symbian OS is written in C++ language for efficient utilization of hardware resources and limited memory constraints. (Source: http://itu.dk/courses/ISOM/E2005/Nokia_and_Symbian_OS%5B1%5D.pdf)

4. MOBILE FORENSICS INVESTIGATION PROCESS

Though there is a very small line of difference between the computer system and a mobile device but the tools used for the mobile forensic are totally different. For instance most of the operating system of the mobile phones is open like Android but in a feature phone it is closed. And it becomes difficult to understand the file system and structure of such phones.

There are diverse forensic tools available for the examination and analysis of mobile device. Some of them are commercial and open forensic tools and some non-forensic tools which are mainly used for device management, testing and diagnostics. The main aim behind designing these tools was to acquire data from the internal memory of mobile phones.

Before understanding the various steps in mobile forensic investigation, we will first discuss about the tool classification system which is based on the type of data extraction methods used. It has five levels from Level 1 to Level 5 and as the level of data extraction increase from bottom to top the methods involved becomes more technical, invasive, tedious and expensive.

4.1 Tool Classification System

Manual Extraction

This method refers to acquiring the data from the mobile device. The content can be on the LCD display which requires human intervention to operate the keyboard or the touch screen to get the information. Manual extraction become difficult when the touch screen is damaged or the keyboard is missing. Also it is difficult to retrieve data if it is deleted. And if the device are configured with the languages not known to the examiner and it becomes difficult to navigate the menu.

Logical Extraction

This method is accomplished by either using wired connection like a USB or wireless connection like IrDA, WiFi or Bluetooth. The investigator should know the issues related to the specific connectivity method as different connection types, deal with data in a different way. For instance all the connection types have a protocol associated with it and these protocols deals with data extraction in a different way. Logical extraction consists of series of commands which are exchanged over an interface set between the computer and the mobile device.

Physical Extraction

This method deals with the raw information stored in the flash memory of the mobile device. It provides direct access to the forensic investigator to this information. The most promising part of this method is the ability of the tool to parse and decode the captured image and make this information available to the examiner with the logical view of the file system. Many techniques are available to physically extract an image from the mobile device. One of the techniques is to upload a modified boot loader or some similar kind of software into the RAM and capture the flash memory and send it to the forensic workstation. Another method is the Joint Test Action Group (JTAG). In this technique the microprocessor of the mobile device is accessed to produce an image.

Chip-Off

Chip off requires physical removal of the flash memory for the acquisition of the data directly from the mobile phone. After extracting the data from the flash memory, examiners create a binary image of the removed chip. Here in order to create a binary image of the chip, reverse engineering is performed on the wear levelling algorithm. After all this is finished, then data is analyzed for the information gathering. The biggest challenge of chip-off is that, it requires extensive training to successfully perform the extraction.

Micro Read

This method requires recording the physical observation of the gates (NAND or NOR) on the chip by using electron microscope. It requires an extreme level of technicalities and so it is used only for high profile cases equivalent to national security crisis.

4.2 Investigation Steps

Preservation

This is the first and the basic step that provides an insight of how to deal with the mobile devices. It mainly consists of searching for the information, recognizing the evidence traits, documenting the data found and collecting electronically based evidences. It is very important to preserve data so as to ensure that it is successfully presented in the court of law.

There are three basic steps involved:

Securing and Evaluating the Scene: This step ensures that the mobile device found is with proper authorizations for beginning the investigation. If the device is not handled properly then it may cause data loss. Also other biometric investigation procedure like fingerprinting or DNA tests are carried to establish the link between the device and owner, so if the device is not handled properly physical evidence may also get contaminated.

Documenting the Scene: Documenting includes keeping the record of all the visible data on the mobile device. This is done mainly for the non-electronic evidence such as invoices, manuals and packaging material. This provides useful information like capabilities of the device, the network used, account information and PIN codes.

Isolation: Isolating the mobile devices from the other devices used for data synchronization is important to keep new data from contaminating existing data. For instance if the mobile phone is found in water and then if it is connected with a personal computer then pulling a plug from the computer overwrites the data or the data is lost.

Acquisition

This is the process of cloning the device or generating its mirror image in order to collect the information from mobile device. Acquisition has an added advantage that it saves the loss of information due to battery depletion, damage etc. This

step begins with identification of mobile device, the type of operating system, device characteristics, the interface the device is using and device label.

Examination and Analysis

Examination process reveals the hidden or the obscured data of the digital evidence. It takes the copy of the evidence which is acquired from the mobile device. It also reduces the data by separating the relevant information from the irrelevant. Mobile phone manufacturers provide a set of features to identify the type of data while gathering the information. The features are like Personal Information Management (PIM), applications, messaging, e-mail and browsing. With the help of these features set potential evidence could be obtained which further may help in the investigation process like:

Date/time, language, and other settings
Phonebook/Contact information
Calendar information
Text messages
Outgoing, incoming, and missed call logs
Electronic mail
Photos
Audio and video recordings
Multi-media messages
Instant messaging
Web browsing activities
Electronic documents
Social media related data
Application related data
Location information
Geo location data
Subscriber and equipment identifiers

Reporting

Lastly, reporting is the process of preparing a document which summarizes all the steps carried out during the investigation process. It depends on maintaining a careful record of all actions and observations describing the results and examinations and explaining the inferences drawn from the evidence. A good report relies on the solid documentation, notes, photographs and tool generated content.

5. MOBILE FORENSICS TOOLS

The number of mobile handsets are increasing day by day. What further complicates the forensics investigation process is change in technology. The tools being used by forensic experts may not be compatible with the latest mobile device and developing a new forensic tool becomes a challenge. It becomes necessary to constantly update the database of the devices supported by the forensic software. The following are a list of mobile forensics tools:

Table 3. List of Mobile Forensic Tools

Mobile Forensics Tools (Commercial)	Mobiledit Forensic iXAM MSAB XRY CellDEK TEK Oxygen Forensic Paraben DDS Cellebrite UFED
Mobile Forensics Tools (Free)	Mobiledit Lite Bitpim Autopsy

The results explained in the next section are obtained from Mobiledit Lite and Autopsy for the device Nokia E71 with Symbian OS as the operating system. Bitpim has not been discussed as the enlisted device is not supported by it.

6. EXPERIMENTAL RESULTS

6.1 Mobiledit Lite 7.8.2.6050

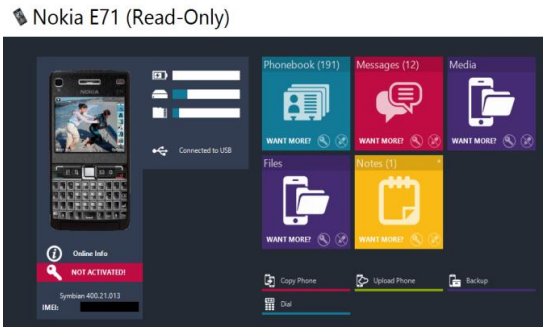

Figure 1. Device Information in Mobiledit Lite

Mobiledit Lite is an open source tool for mobile forensics using which address book, SMS, Media files, Notes and Files can be analysed. Backup of the phone can be created so that further analysis is not carried out on the evidence itself. The software is able to identify the IMEI (International Mobile Equipment Identity) number of the mobile phone. It has been blacked out in the image for security purposes. These are the features provided by the free version.

Additional facilites for authentication bypass, Backup encryption, Cloning SIM Card and retrieval of Application data are provided in the commercial tool. (Source: http://www.mobiledit.com/forensic)

6.2 Autopsy 3.1.2

Autopsy is an open source digital forensic tool that can be used for investigating cyber-crime. The purpose of the tool is to identify all possible pieces of information which could be useful for further forensic examination. Case management, integrity of disk image, search, time-line analysis are some of the major functionalities of this tool.

Using Autopsy, mobile phones can be examined for retrieval of SMS, Contacts, Media files, Calendar and Notes.

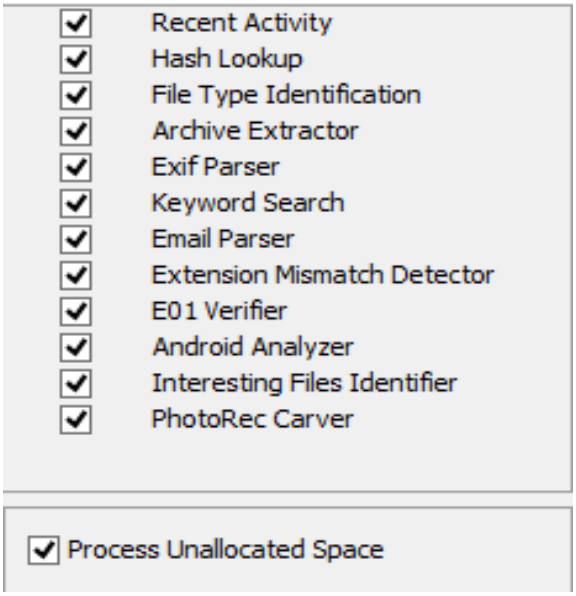

Figure 2. Configuration of Ingest modules

Multiple ingest modules are executed simultaneously for better utilization of multi core systems. (Source: http://www.sleuthkit.org/autopsy/fast.php) The reports can be generated by the user in HTML, XLS and Body file format. The report contains the following:

1. Information regarding File Systems (File attributes such as extension, is deleted, last accessed, last modified, hash value)

2. Information regarding Web Activities (History, Cookies, Web Search and Downloads)

3. Miscellaneous types (SMS, Location, Call logs, Contacts and Media files)

This report can be used in documenting evidence related information or supporting evidence. Detailed analysis of the files is also possible. The use of Autopsy can be accompanied with the Sleuth Kit for additional functionalities.

6.3 Case Study

These results have been obtained for Nokia E71 device using the tool Autopsy to gain more information regarding deleted file systems. We have recovered the contents of a deleted Microsoft PowerPoint file. The file type has been correctly identified as pptx. Each artifact is assigned a unique identifier. For the PowerPoint File Seminar.pptx, we have obtained the date and time when it was created, last accessed and modified. The MD5 value for the file has also been calculated to avoid any integrity conflicts.

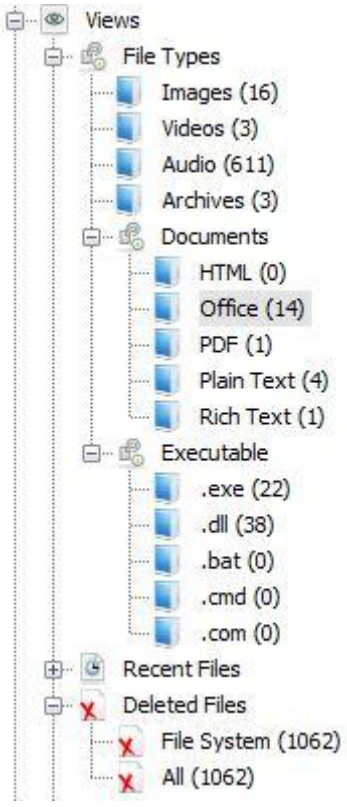

Figure 3. List of files

Name	/img_D:/Seminar.pptx
Type	File System
Size	1459626
File Name Allocation	Unallocated
Metadata Allocation	Unallocated
Modified	2012-11-03 12:28:44 IST
Accessed	2012-11-03 00:00:00 IST
Created	2012-11-02 22:43:53 IST
Changed	0000-00-00 00:00:00
MD5	35a75a442bfa0eeefb0936ae495e41ff
Hash Lookup Results	UNKNOWN
Internal ID	2934

Figure 4. Metadata of deleted file

The Timeline Analysis shows the files accessed during the given timeframe. This is useful for event reconstruction during forensics investigation. From timeline analysis, we can obtain a graphical output of the types of resources present in the mobile device in the form of documents or media files with respect to time. The timeline analysis displays the events occurred in a particular time frame. This helps not only in identifying suspicious/anomalous activities, but also the time range in which the incident or event occurred.

6.4 Comparison of Open Source Mobile Forensic Tools

The following is a comparison table of features of the two mobile forensics tools discussed. Depending on the type of evidence to be extracted and analyzed, the appropriate tool can be chosen.

Table 4. Comparison of Open Source Mobile Forensics Tools

Parameter	Mobiledit	Autopsy
Operating System platform	Windows XP/ 2003/ Vista/ Windows7	Windows, Linux and OSX
Supported device	Iphone (iOS 3.0 or higher) Android Symbian Windows (Limited to contacts and media files)	Disk images Local drive, Folder/ Directory
Connection via	USB Cable, WiFi, Bluetooth, Infrared	USB Cable
IMEI Number	Yes	No
Physical Data Acquisition	No	Yes
Logical Data Acquisition	Yes	Yes
Type of evidence recovered	SMS, Contacts, Files, Media	SMS, Contacts, Files, Media, Metadata
Output format	-	Text, XLS, HTML

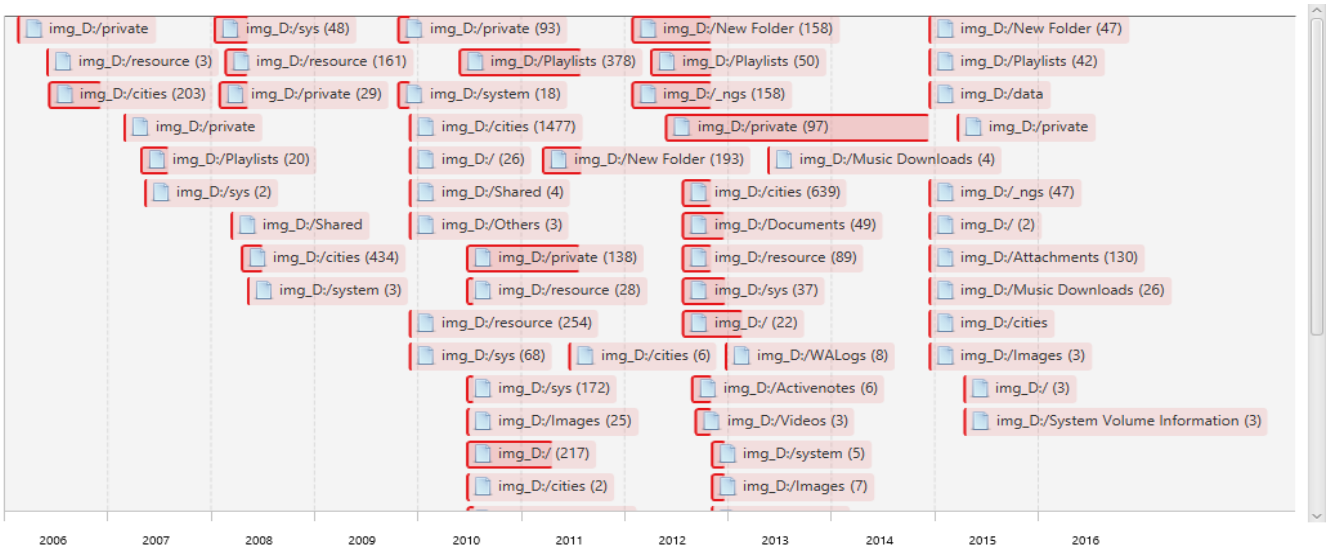

Figure 5. Timeline Analysis

7. CONCLUSION

With the help of open source digital forensic tools like Mobiledit Lite and Autopsy 3.1.2, details such as SMS, Call registers, Images, Songs, Videos and Files can be stored for further investigation. Mobiledit Lite comes with write blocker (read only) feature so as to ensure the integrity of the mobile phone is maintained and the evidence is not contaminated. Mobiledit Lite and Autopsy 3.1.2 alone are not sufficient to recover deleted items. Other open source tools or commercial tools can be used along with them for additional functions such as authentication bypass, SIM cloning and Retrieval of browsing internet data. Using Timeline Analysis report of Autopsy 3.1.2, the sequence of events can be established and useful in event reconstruction.

8. ACKNOWLEDGMENTS

This paper was taken as part of study for forensic science investigation and Mobile Forensics. We would like to express our sincere thanks to HOD and guide in Computer Science Engineering Department, Institute of Technology, Nirma University for many fruitful discussions and constructive suggestions throughout.

9. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .

[2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

[10] Yates, I. I. "Practical investigations of digital forensics tools for mobile devices." 2010 Information Security Curriculum Development Conference. ACM, 2010.