Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.74 – 79

SURVEY ARTICLE

Cyber Forensics in Kerala

Arunima S Kumar

Mar Baselios College of Engineering & Technology, Thiruvananthapuram, Kerala, India
arunima3032@gmail.com

Abstract— Computers and mobile devices have created a niche for themselves in the digital communication stratosphere. With the advance of technology, the power of these devices has increased leaps and bounds. Due to this growing popularity, computers and mobile devices have plunged into criminal activities also. Drug dealers, rapists and murderers across the State have been caught based on the electronic devices they carry around.

Cyber Forensics deals with the application of investigation and analysis techniques to gather and preserve evidence from a computing device in a method accepted by the court of law. Mobile Device forensics is an evolving form of cyber forensics. New models of mobile phones are released every few months and thus its usage has also increased tremendously – both for good and bad purposes. This scenario poses new challenges for forensic examiners because acquiring tamper-free data from a mobile device is of great importance in crime investigations. Such data resides at different locations in a mobile device such as handset memory, attached memory cards, call records, SMS, calendar entries, installed applications etc.

This paper deals with the study of forensic tools used for investigation of cyber crime in Kerala. The paper discusses the capabilities and shortcomings of the forensic tools under study. An enhancement is proposed for the currently available tools, to make them a comprehensive set of tools with a set of features that combats a wide range of cyber and mobile device crimes.

Keywords: mobile device forensics; forensic tools; digital evidence; data acquisition; storage media; data extraction; crime investigation

I. INTRODUCTION

The twenty first century awoke to the wakeup call of Information – Communication Technologies (ICTs). With the advancement of ICTs, the power of the computers and mobile devices has increased rapidly. They have become an intricate part of our daily lives. The prominence of ICTs in all walks of life has made our democratic and constitutionally bound society into an increasingly crime-prone zone. No doubt these technologies have elevated crime rates and have given birth to a gamut of 'innovative" crimes.

Cyber crime is the latest and perhaps the most rampant evil in this era of criminalisation. In this contemporary scenario where everything from small gadgets to nuclear plants is being operated through computers, cyber crime has assumed threatening ramifications. "The

modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[1]

The Information Technology (Amendment) Act 2008 under the Constitution of India has categorised cyber crimes in two ways:

- The computer as a target: using a computer to attack other computers. e.g. hacking, DOS attack etc.
- The computer as a weapon: using a computer to commit real world crimes. e.g. cyber terrorism, pornography, etc.

According to this Act, all cyber crimes are punishable under the Indian Penal Code. [3]

II. CYBER FORENSICS & CYBER FORENSICS TOOLS

Cyber Forensics or Computer Forensic Science or Computer Forensics is a branch of digital forensic science pertaining to legal evidence residing in computers and digital storage media. It deals with acquisition, verification, analysis, preservation and documentation of evidences extracted from and/or contained in a computer system or network and other peripherals. Computer forensics is done in a way that adheres to the standards of evidence that are admissible in a court of law. "Two distinct components exist in the emerging field of computer forensics. The first component deals with gathering computer evidence from computer media seized at the scene of crime. This involves imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes, analyzing the data for evidence and reporting the evidence in a manner acceptable to the court. The second component is Network Forensics which involves gathering digital evidence that is distributed across large-scale complex networks." [2] Thus computer forensics is techno-legal in nature.

Special programs for acquiring and analyzing storage media as a whole are called Cyber Forensic Tools. These tools can be either hardware tools or software tools. In order to verify a tool is forensically sound, the tool should be tested in a mock forensic examination to verify the tool's performance. There are government agencies such as the Defense Cyber Crime Institute that accept requests to test specific digital forensic tools.[3],[11] Some forensic tools that adhere to the forensic soundness are EnCase, Forensic ToolKit (FTK), PTK Forensics, Oxygen Forensic Suite, Belkasoft Evidence Center etc.

A computer forensic expert is engaged to carry out the examination process in a court approved format. They employ state-of-the-art tools and methodologies in the extraction and analysis of data from storage devices. "The goal of a forensic investigator is to obtain evidence utilizing the most acceptable methods, so that the evidence will be admitted according to law in the trial. Obtaining a judge's acceptance of evidence is commonly called admission of evidence. Evidence admissibility will require a lawful search and the strict adherence to chain of custody rules including evidence collection, evidence preservation, analysis, and reporting."[4]

III. FORENSIC TOOLS USED FOR CRIME INVESTIGATION IN KERALA

A number of forensic tools are available in the public domain. But the selection of forensic tools to be used for an investigation depends upon the nature of the crime. But the fact is that there is no universal cyber forensic tool which could be used in the investigations of different types of cyber crimes.[8],[12],[13] As per National Crime Records Bureau statistics 2012, Kerala ranked fourth among the States that have reported maximum cybercrimes with 312 cases in the year 2012. This indicates that cyber crimes are increasing at an alarming rate in the State.[15]

The analysis of a crime scene by an investigating officer starts with the seizing of the evidences. In this phase, the officer takes the hash value of all the evidences. This hash value and the time of seizure are of great importance. After the seizure, all the evidences along with

the case details are submitted before the court. The court forwards the evidences to the Forensics Science Laboratory for further forensic analysis of the evidences. The analysis is done on the basis of 'forwarding note' submitted to the court by the investigating officer. At this point, the forensic expert performs the acquire operation on the seized storage media. It is always advisable not to work with the original copy of the seized components. Hence, the forensic expert creates a shadow or image of the seized media and performs sector by sector analysis on it.[5],[7] Meanwhile, the MD5 hash computation algorithm will be performed on the disk read. All the information will be saved into the report file for legal use. During this process, the forensic expert verifies the integrity of the data acquired by him and the date obtained during the seizure by the investigating officer. The hash values of the images obtained during the seizure are compared with the corresponding hash values obtained during acquisition. If there is a mismatch between the hash values, it can be concluded that the data is being tampered.[14] The seize and the acquire procedures can be done together at the scene of crime with the presence of a forensic expert.

Due to security reasons, the names of the cyber forensic tools used by the Forensic Science Laboratory and the Cyber Police Station, Kerala are not revealed in this paper. The tools used to extract data from storage media like hard-disks, USB drives etc were different from tools used to extract data from mobile devices. The cyber forensic tools used in this paper were chosen because of their usage in the investigation of cyber crimes in Kerala. Let the tools under consideration be named as Tool A, Tool B, Tool C and Tool D. Among the tools, Tool A was found to support the data acquisition and analysis of storage media such as USB drives hard-disk, CD, Floppy-disk etc. Tool B supports the data extraction of storage media and mobile devices. Tool C and Tool D are exclusively used for the extraction and analysis of data from mobile devices. All the four software uses MD5 Hash Algorithm for ensuring data integrity.

A comparison between the tools A, B and C is made based on their mobile device forensics compatibility in Table II and Table III. The mobile device used for the comparison is an Android smartphone namely Samsung Galaxy SII. Table I shows the specifications of the selected smartphone. The comparison is done based on the data types that are commonly retrieved by the three tools.

TABLE I
SPECIFICATIONS OF SAMSUNG GALAXY SII

Manufacturer	Samsung
Operating System	Android 4.0.4 (Ice-cream Sandwich)
RAM	1GB
Internal Memory	16GB
External Memory Card	No
Chipset	Exynos
CPU	Dual-Core 1.2GHz Cortex – A9

Logical extraction and Physical extraction of the mobile device should be done to extract maximum information from it. Logical extraction acquires information from the mobile device using the device manufacturer's interface for synchronising the device with the computer. This method does not retrieve deleted information. All the 3 tools support logical extraction. Table II shows the result of the logical extraction of the smartphone. It was found that tools B and D could not extract overwritten files and the extraction did not cover all the locations where data could be found in a mobile device.

TABLE II
LOGICAL EXTRACTION RESULTS

Data Type	**Tool B**	**Tool C**	**Tool D**
Contacts	150	320	180
Call History	212	212	212

SMS	1550	1550	1550
MMS	14	14	14
E-mail	7	9	Unsupported
Calender entries	45	45	45
Bookmarks	Unsupported	11	Unsupported
Web History	81	191	Unsupported
Images	1089	1100	98
Video files	5	7	0
Audio files	220	115	0

Physical extraction involves making a bit-by-bit copy of the entire physical storage. This method requires direct access to the file system of the mobile device since it acquires deleted files also. Table III shows the result of the physical extraction of the smartphone. It was found that only Tool C supports physical extraction. The figures within square brackets refer to the number of deleted items retrieved. Eventhough Tool C could retrieve deleted messages, it reported problems while extracting deleted messages from mobile devices prior to the number of days specified by the 'log duration' parameter in device' log application. Even if the messages got extracted successfully, only part of the message text was retrievable.

TABLE III
PHYSICAL EXTRACTION RESULTS

Data Type	**Tool B**	**Tool C**	**Tool D**
Contacts	Unsupported	143 [18]	Unsupported
Call History		0	
SMS		1550 [250]	
MMS		14	
E-mail		20	
Calender entries		89	
Bookmarks		14	
Web History		220 [47]	
Images		8750 [2413]	
Video files		11[5]	
Audio files		150[12]	

Tools A and B takes more processing time while checking for encrypted files from a large evidence-file-set. Tool A has the facility to recover deleted partitions, but the overheads are very high while loading the recovered partitions. All the four tools provided the "auto-save" facility whereby the findings of an analysis session got automatically saved into the destination media/folder periodically. File searching and keyword searching, based on user defined filters is also available in these tools.

Among the tools studied, Tool A was found to be a better tool with the following additional features.

- Perform self-integrity check while loading
- Provides the facility of previewing of the storage media before seizing or acquiring
- Creation of customised Hash Set Library
- Anti-Forensic detection
- Scripting of customised programs which are specific to a case
- Retrieval of overwritten files
- Unicode support & Indian Language support
- Presentation of all picture files in the evidence-set in a single window
- Windows Registry and configuration files viewer with search
- Search facility with Unicode characters
- Analysis report generation during all stages

IV. PROPOSED SYSTEM

Eventhough Tool A was found to be a better one; it lacks features to support mobile devices. It is clear from Tables II and III that Tools B, C and D do not cover all locations where evidence can be found. Moreover Tool B lacks some features to support computer forensics. The proposed system is a mobile device compatible version of Tool A which facilitates data recovery and analysis of any devices including smartphones, tablets, fablets and other wearable devices.

The main objective of the proposed system is to facilitate forensic analysis of different devices such as hard disks, USB drives, smartphones, laptops, tablets, fablets etc using the principle of disk forensic analysis used in the original version of the tool.

The following enhancements of Tool A are proposed.

- Extension of the data integrity checks to the mobile devices
- Automatic Operating System (OS) detection of the mobile devices
- Reviewing the data acquisition in real time
- Menu driven user-interface to facilitate the selection of the area of interest
- Hash Library containing hash values of system files and other standard mobile applications available in the market place or appstore
- Hash Library of common spywares
- Multi-node network version of the tool
- Scripting facility to customise the search query
- Facility to access device data directly during extraction without using any data synchronisation applications
- Support for wired, wireless, infrared, Bluetooth and Near Filed Communication (NFC) connections
- Support for different platforms and OS such as ios, Android, BlackBerry, Symbian, Windows etc and common handsets like Nokia, Apple, Google, Samsung, Sony Ericsson, Micromax, Motorola, LG, HTC, HP, Acer, Panasonic etc.
- Compatibility with Windows XP, Windows Server 2003, Windows 98, Windows 2008, Windows 7 and Windows 8 irrespective of whether it is 32 bit or 64 bit.
- Provision to extract evidence from all possible locations in a mobile device. Evidences could be available in PhoneBook, Calendar, Tasks, Notes, Messages (including custom SMS folders), Logs, File Browser, TimeLine, Geo Positioning, Web Connection and Location services, Applications, Web Browsers, Dictionaries, Skype, Google Services (Google Maps, Google Calendar, Gmail, Google+,etc.), Yahoo Services(YMail, Yahoo Messenger, etc.), Social Networks(Facebook, Twitter etc.), Messengers (GTalk, Sype,etc.) etc.
- Aggregate view of all contacts available in the device

V. FUTURE WORK

Recently, some mobile phone manufacturers emulate all facets of a branded phone's appearance to make it appear as genuine. This makes it very difficult for the forensic experts to identify whether a phone is fake or genuine. Many of such counterfeit mobile phones will not have the International Mobile Equipment Identity (IMEI) number. They may even use a fake number.[10]

The data extractions from such mobile phones pose a challenge to the forensic experts. Acquisition and analysis of such phones are really difficult because they use custom designed OS and it is the biggest threat to security.

Tool A can be further extended to handle such devices. If this is achieved, it will be a revolutionary step in the field of mobile device forensics.

VI. CONCLUSION

Cyber crimes using mobile devices are increasing at a skyrocketing pace. This scenario poses new challenges for forensic examiners in acquiring tamper-free evidence from mobile devices, which is of great importance in crime investigations. But mobile device forensics seems to evolve at a slow pace. "For this to catch up with the release cycle of mobile devices, more comprehensive and in depth framework for evaluating mobile forensic tool kits should be developed and data on appropriate tools and techniques for each type of device should be made available in a timely manner."[4]

The paper discussed four different forensic tools that are used for the investigation of cyber crimes in Kerala. But there are some pitfalls and shortcomings for these tools. An enhancement of these tools is proposed which makes it feature rich enough to tackle the forensic analysis of the current cyber crimes and those in the near future effectively.

ACKNOWLEDGMENT

I hereby express my deep and sincere gratitude to my guide, Prof. Raju.K.Gopal for all the help and guidance offered to me to make this study a fruitful one. I extend my sincere thanks to Mr.Sreejith IPS, Deputy Inspector General of Police and Chief Investigation Officer, Human Rights Commission, for all the support rendered to me to make this study. My thanks are also due to Mr.Sunil Jacob, Superintendent of Police, Cyber Police Station, Mr. K.L. Thomas, Associate Director, Cyber Forensics Wing, CDAC, Thiruvananthapuram, and Mr. Vinod Kumar, Cyber Police Station, for all their help and support in this venture.

REFERENCES

[1] Stefan Savage and Fred B. Schneider, Security is Not a Commodity:The Road Forward for Cybersecurity Research, Version 4. [Online]. Available: http://www.cra.org/ccc/files/docs/init/Cybersecurity.pdf

[2] John R. Vacca, "*Computer Forensics: Computer Crime Scene Investigation*," 2nd ed., Charles River Media, 2005, p.35-36

[3] (2013) The Indian Cyber Laws website. [Online]. Available: http://www.cyberlawsindia.net/

[4] David W. Bennet (2011). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigation. [Online]. Available: http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

[5] CDAC Official Website. [Online]. Available: http://www.cdactvm.in/

[6] Jerry Li (2003). MD5 – Message Digest Algorithm. [Online]. Available: www.cs.sjsu.edu/faculty/stamp/**CS265**/projects/papersSpr03/MD5.ppt

[7] Jack Euan Ross McMillan, William Bradley Glisson and Michael Bromby, "Investigating the Increase in Mobile Phone Evidence in Criminal Activities" in 46th Hawaii International Conference on System Sciences, 2013.

[8] Amjad Zareen and Dr. Shamim Baig, "Mobile Phone Forensics – Challenges, Analysis and Tools Classification," in Fifth International Workshop on Systematic Approaches to Digital Forensics Engineering, 2010.

[9] Det. Cynthia A. Murphy, "Developing Process for Mobile Device Forensics", version 3, 2012

[10] Secure India – Mobile Phone Forensics Website (2013). [Online]. Available: http://www.secureindia.in/?page_id=27

[11] Rick Ayers, Wayne Jansen , Ludovic Moenner and Aurelien Delaitre, "Cell Phone Forensic Tools – An Overview and Analysis Update", 2007

[12] K.K. Arthur and H.S. Venter, "An Investigation into Computer Forensic Tools"

[13] Sean C. Sobieraj, "Mobile Device Forensics Case File Integrity Verification," Master of Science thesis, Purdue University, West Lafayette, Indiana, May 2008.

[14] Shira Danker, Rick Ayers and Richard P. Mislan, "Hashing Techniques for Mobile Device Forensics," *Small Scale Digital Device Forensics Journal*, vol. 3, no. 1, June 2009.

[15] National Crime Records Bureau Website (2013). [Online]. Available: http://ncrb.gov.in/CD-CII2012/Additional_Tables_CII_2012/Additional%20table%202012/Cases%20registered%20under%20Cyber%20crime%20-%202012.xls

