Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 11; April-June, 2015 pp. 42-47
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Digital Evidence–Technical Issues

Satish Kumar

Panjab University Regional Campus, Hoshiarpur, Punjab,India
E-mail: satishnotra[at]yahoo.co.in

Abstract—*The evolution of digital computer and Internet technology has given birth to digital information that is created intentionally or automatically by a computer or its associated devices during computing or communicating process. This has further originated various applications such as e-governance, e-commerce, e-payment etc where massive digital information are generated, processed and transcribed daily. This is also a new place of carrying criminal activities as millions of people are using this technology. A criminal may leave evidence in the form of electronic record on the devices it is using at the time of committing crime or involved with crime. The criminals may use various software or hardware tools to destroy such evidences. The investigating agencies have to face various challenges starting from collection of evidences to the final production before the court. This paper covers the value of the digital evidences as per Indian Law and their admissibility in court. The most undesirable fact about the digital evidence is that these can be altered or deleted intentionally or un-intentionally. One can even intentionally hide data on a disk for its own reason. The computer experts have designed software utilities to recover data in such situation. The various such software have been discussed in briefed. At last a look at signature has been briefed.*

Keywords*: Electronic Evidance, IT Act 2000, Data destroying, Data Recovery, Data Imaging, Digital Signature.*

1. INTRODUCTION

Acrime is culpable act banned by law and penalized by a state. It is a harmful act or omission against the public which the states wish to prevent. The decision regarding a crime, whether it is committed by someone (offender) or not, is made on the basis of evidences, these provide reasonable reliable information that gives more reliable/ accurate picture of a crime (to the court, which otherwise is as strange as a layman to the real happening, except the fact that it has knowledge and can apply to the present circumstances).

The Indian Evidence Act, 1872 is the Indian Law of Evidence. Among the various types of evidences, the physical evidences such as body fluid, hair, blood, saliva, clothes, hoes, socks, locket, weapon etc. are significant. This type of evidence can help the experts to decide and /or restructure the events and components of a crime. Direct and circumstantial evidence is given importance over Hearsay Evidence.

The digital evidences are more relevant in the situation the majority of people are making use of digital device for their daily use that may be the source of crime. The investigation or legal dispute also involves some kinds of scientific and digital evidence *i.e*. the electronic record that have been created through a computer intentionally or have been created automatically by a computer or its associated devices. The digital evidences are not only used in cyber related crimes but these are useful to solve other crimes too. In addition to this, the various fundamental questions related to the crime can be resolved using digital evidence. The various issues such as who is crime perpetrated, who contacted whom, where and when based on the sequence of events available in source and destination data of digital evidence.

The Indian IT Act 2000 provides the legal recognition of electronic records and digital signature. The Indian IT Amendment Act, 2008 provides the admissibility of evidences produced through communication devices. There are many sources of digital evidence and these ranges from a tiny SIM card to online server. The most important fact about digital evidence is that they can be distorted, destroyed and distributed worldwide easily. The investigating agencies are facing a number of challenges while collecting the digital evidences related to cyber related criminal activities worldwide.

This paper discusses the provision of Indian law regarding admissibility of digital evidence. The various source of digital evidence and the software/hardware used to collect and preserve the digital evidences are also discussed. The digital evidences can be deleted or destroyed. The various software utilities used to recover these evidences are also discussed. A criminal can deliberately hide data using some data hiding software or hardware techniques. The hardware and software utilities used to hide and recover such data are also discussed. The digital signatures are authentic, un-forgeable, not reusable, unalterable and non-repudiated. The validity of digital signature and its issuance authority in Indian context is also discussed.

2. DIGITAL DATA AND IT ACT 2000

Information Technology Act 2000 provides legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communications which involves the use of alternates to paper-based methods of communications and storage of information, to facilitate the electronic filling of documents with the Government agencies [1]. The Section 3 in the Indian Evidence Act, 1872 allows the evidence in oral or documentary form only. This has been amended to include the evidences in electronic form too. Section 4 of the Indian IT Act, 2000 provides legal recognition to electronic records and Section 5 provides legal recognition to digital signatures [2]. As per Section 2(*t*) of Indian IT Act 2000, "electronic record" *i.e*. the data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche are admissible as an evidence. As per Section 2 (*r*) "electronic form" *i.e*. the information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device are admissible as evidence. As per Section 2 (*r*) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche[3]. Similarly, as per Section 2 (*p*) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3[4].

The Indian IT Act 2000 is again amended in 2008 to include the admissibility of evidences produced through communication devices. As per Section 2(*ha*) of Indian IT Amendment act 2008, the evidences recorded\produced through the cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image are also admissible[5]. Section 69 of Indian IT Amendment act 2008 confers authority to the Government to issue directions for interception or monitoring or decryption of any information through any computer resource, Section 69A confers authority to the Government to issue directions for blocking for public access of any information through any computer resource and Section 69 B confers authority to the Government to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security[6]. As per Section 2 (*nb*) "Cyber Security" is protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

As far as admissibility of digital evidence is concerned, a new provision section 65A, introduced to Evidence Act under second schedule to IT Act, provides that the contents of electronic record may be proved in accordance with the provisions of section 65B which states as any electronic record is deemed to be a document admissible in evidence without further proof of the original's production, provided that the conditions 65B (2) to (5) are satisfied. For more details see [1,7].

An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible [8]. Digital Signatures are legally admissible in a Court of Law, as provided under the provisions of IT Act, 2000.

3. DIGITAL DATA – A LOOK

The digital evidence is any digital data or information that is stored, transmitted or received through an electronic device such as computer, laptop, tablet, mobile, telephone, pager etc and it is very important being containing some proof of some sort of crime, affirmation either oral or printed text or an act that is helpful for resolving crime related issues. In simple term, Digital evidence is any digital information that may be used as evidence in court in favour or defence of a case. The various devices attached to the computer system such as hard drives, Solid State Drives (SSD drives), portable drives/storage -USB flash, CD/DVD disks, SD cards etc and external devices with storage capability may be the source of digital data. The information or data of documents, images, videos, voice etc in encrypted or unencrypted form, Internet browser history, log files on a server or intermediate server or router, chat logs, e-mail and e-mail attachments, Virtual Private Network, encryptions available on hard-drive or portable drive of a system. Very small storage device like thumbnail such as memory card, SIM card, micro-SIM card used with mobile, tablet, laptop, digital camera, digital music player, Personal Digital Assistant may also a source of digital evidence.

The cyberspace is globally spread like a web and the information on it can be transported to any part of the world since there is no boundary between the countries on cyberspace even though each and every country is governed by its own Law. The law of a nation is limited to its boundaries and one nation has to respect the sovereignty of another. Moreover, there is a complete lack of international cooperation and mutual legal assistant in combating cyber related crimes and this helps the criminals to get escaped unpunished. At the same time social media is an important communication channels among the people worldwide where there is no geographical boundary between the countries. This is not only beneficial for people across world but it also attracts the criminals. The majority of crimes related to cyber space perpetrated on social media. Pros side of social media in taming crime is that it helps to trace the criminals by locating proper digital evidences from the appropriate device on Internet. The con side is that the digital evidences can be destroyed and distorted. Cybercrime falls into three categories [9]: (1) a computer is the target of criminal activity; (2) the computer is the tool used or is integral to the commission of the crime; and (3) the computer is only an incidental aspect of the crime.

Apart from some procedures to ensure the integrity and authenticity of digital evidences as allowed or permissible by Courts, the investigating agencies are facing a number of challenges while collecting the digital evidences related to cyber related criminal activities. The major sources of challenges are [10, 11, 12]: 1) The crime related data may be distributed across the network\cyberspace irrespective of physical boundaries of different countries; 2) Digital data on a computer may be altered or deleted deliberately or accidentally. Moreover, in temporary memory it stays for a limited period only as and when it is under process \transfer. Similarly the network traffic is transient that can be captured at transfer time only; 3) Extracting and analyzing effective data from huge amount of data collected from different computers on a network is a tedious task; 4) Lack of technical expertise while dealing with the number of computers, in the form of different network hardware and software implements, involved with the malicious activities. 5) Lack of legal expertise from the start of collecting the evidence to proving it before the court. The last two points requires to adhere the following: *a*) legality principles while collecting evidence, *b*) security and integrity principles while storing or preserving information and authenticity principle while making the chain of custody.

4. DIGITAL DATA – SIGNIFICANT ISSUES

4.1 Authenticity & Integrity of Digital Data

The investigating agencies or cyber forensic experts dealing with electronic data usually faces many problems right from its collection to final production before court. In the process of gathering digital evidence, the investigating officer may require seizing of storage media, monitoring or tapping of network traffic and/or making of digital copies of detained data. The challenges are related to collection, maintenance, recovery, security, authenticity and integrity of digital record.

The digital data in form of evidence may be admissible by a court only if there is evidence that the collection of information contained in electronic record have been created through a computer intentionally. It means the digital record in the form of a letter, a message, a document, an advertisement, a memorandum, a deal, voice record, and video record which proves that the crime perpetrated has some sort of relation with them may be permissible by court as evidence. Some digital evidences are evolved as a result of computer/communication system's processes. These are not created by the criminal directly but are automatically generated by the system. In such digital evidences the credibility of correct functioning of computer system that has created such digital evidence might be questionable in a court. The records belonging to this category are: chat room logs and logs or records available with ISP (Internet Service Provider), logs of data collected from a server or an intermediate server or router on network, electronic banking record, cell tower record, telephone\mobile toll records, Email header information, GPS (Global positioning system) records etc.

The authenticity and integrity of the digital evidence may be under question while admitting the digital evidence in court. The authenticity of digital evidence means, whether the evidence has been originated from the purported source? The integrity means accuracy and consistency of *data i.e.* whether the evidence is same as it is collected from the purported source or it has been deliberately changed?

4.2 Destroying and Distortion of Digital Data

The digital records can be altered or deleted deliberately by a criminal. There may be situation that the record is altered or deleted accidentally while collecting the evidences or its improper handling or any another reason. For example Windows OS records number of user activities in log files. Internet browser records the track of visited pages in Internet History. These logs or Internet history, cookies, temp files and saved form data can be deleted by anyone easily using various options available in OS\browser. For example "regeditor" in Windows OS can be used to delete Search history & Run history. Moreover, history information stored in the registry such as Opened & Saved documents, Search history & Run history can be deleted using Spybot - Search & Destroy tool actually designed to detect and remove spyware is easily available. Some virus, worms and Trojan horse can destroy digital data. The Eraser[13] allows anyone to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

Actually, multiple index.dat files are hidden files on your computer that contain information of all the Web sites that one have ever visited and are not deleted by clear history and delete temporary files. Similarly, Index.dat Suite[14], Ace [15], CCleaner[16], OSPC:Privacy Cleaner[17], IE Privacy Keeper[18], index.dat Analyzer[19], PrivacyMantra[21], etc utilities can be used to delete the hidden index.dat files. Keeping in view the privacy of mobile users some apps such as CCleaner[16], Clear Master[21], History Eraser etc are easily available in market to destroy digital evidences on mobiles.

The investigator must be cautious and not allow any person to access, move, or remove the crime related computer and associated components till all evidences have been collected and stored on a separate device. The investigator must check hardware, software, document files, image files, video and audio files, encrypted files, web cam snap shots, backups and log files related to the computer under investigation.

5. SOFTWARE TOOLS\UTILITIES

5.1 Disk Imaging or cloning

It is desirable to make complete bit stream image of the media containing electronic record to avoid its deletion or modification. The various disk imaging Tools used by forensic experts are: SafeBack [22] is a utility used to create mirror-image (bit-stream) backup files of hard disks or to make a mirror-image copy of an entire hard disk drive or partition. It is an industry standard self-authenticating computer forensics tool that is used to create evidence grade backups of hard drives; SnapBack[23] is a server based Backup and restore program; EnCase Forensic Version 6 [24], is a software used to analyze digital media and having tools for data actuation, data recovery, preserving and file parsing etc. It has a number of powerful features that facilitate efficient examinations, including recognition of the various files typically associated with Internet and email artifacts; ProDiscover Forensics[25] is a set of computer security tools used to collect, preserve, and analyze computer evidence. It can recover deleted files, examine slack space and access Windows alternate data stream; Forensic Toolkit (FTK)[26] is a software used for computer forensic analysis, decryption and password cracking and has customizable interface, Helix3 Pro [27] is a unique tool with a Live and Bootable side for investigation needs. It can work on multiple platform, Mac OS X, Windows and Linux and is used to make forensic images of all devices, search file systems for specific file types (i.e. Graphic files, Document files, etc) . In addition to this it has many open source forensic applications to assist with data analysis**.** ILook (v8) [28] is an Investigator Forensic Software and it contains many computer forensics tools used to acquire and analyze digital media. ILook has strong processing capabilities including advanced email deconstruction and analysis, thorough and comprehensive indexing capabilities, a wealth of reporting features, and advanced unallocated space data salvaging capability. DIBS RAID (Rapid Action Imaging Device) [29] is light weight unit used to copy hard drives fast. Its average sped of coping is 2.4 GB to 4 GB per minute. It is portable and provided as tough and polythene case. X-Way Forensic [30] can be used to disk cloning and imaging. This tool has ability to read partitioning and file system structures inside raw (.dd) image files, ISO, VHD and VMDK images. It automatically identifies the lost/deleted partitions. With ASR Acquisition and Analysis [31] tool one can acquire and clone a single source to any number of images and devices simultaneously. This enables you to make a backup copy and working copy at the same time. The SMART acquisition is a powerful and flexible options allow you to create pure bit-image copies AND quasi-proprietary formats that support seekable compression. Paraben Forensic Replicator (PFR) [32] is a bit-stream forensic image creation tool that creates bit-by-bit raw DD images of hard drives and related media. With PFR one can create bit-by-bit forensic images, verify your image integrity with hash calculation, document use of write blockers in your report, view an image's contents etc. DCFLDD [33] is enhanced version of dd (GNU Coreutils package) which is often used to create bit-stream image files of media as part of a forensic acquisition process. DCFLDD offers additional features like Hashing on the fly, Image/wipe Verify etc. DEFT [34-35] Digital Evidence & Forensic Toolkit use LXDE as desktop environment and ‘thunar’ file manager and mount manager as tool for device management. CAINE (Computer Aided Investigative Environment)[36] is mainly used to acquire data of a suspected criminal computer and it is also useful as a backup live CD.

It is easier to produce the duplicates of digital data to avoid the risk of damaging the original. The digital evidences can be recovered even if these are deleted or formatted from a disk.

6. DATA RECOVERY

A criminal can be a computer expert who may use a complicated technique to hide his data in unconventional location on a hard disk. The criminals can delete or erase data from a disk. When such acts are committed, the clusters on which the data is stored are not reallocated until new data is written on them. Formatting or repartitioning a disk does not eliminate the data till the clusters are overwritten. A number of software are available to recover data from such unallocated areas. In order to recover accidentally deleted files, the various software utilities used are: Recuva[16], DiskDigger[37], EaseUs Data Recovery[38], Handy Recovery [39], UndeletePlus[40], The Sleuth Kit (Collection of Commands) and Autopsy program (GUI based)[41]. Some other software tools used for this purpose are: R-Studio, SmartUndelete, GetDataBack, FileScavenger, Filesaver, R-Undelete, DataRecovery and many more.

The first 512-byte sector on the drive, called as Master Boot record (MBR), holds the partition table. The MBR keeps track of where the partition is located and the size of each partition. The partition table keeps track of logical hard drive partitions. It may become corrupt due to several reasons. Partition recovery tools help anyone to recover deleted and damaged logical drives and partitions created using OS like DOS, Windows, linux etc. The various such tools available are: Active@ Partition Recovery, GetDataBack, EaseUs Partition Recovery, NTFS partition recovery, Disk Internals Partition recovery etc. Some tools can even recover partitions and these tools are: ZAR Data Recovery, Handy Recovery, Quick recovery for FAT & NTFS etc. The data search tool can even locate the data present in partitioned gap.

One more way to conceal data on a disk is to encrypt it using some password or key. The lengthy passwords formed from the combination of alphanumeric and special characters are difficult to crack but weak passwords are easy to recover. There are many softwares such as Paraben’s decryption collection[42], Passware Kit Forensic, Distributed Network Attack(DNA) [43], Ophcrack [44], L0phtCrack[45], Cain and Abel[46], Data Recovery Pro[47], APASSCRACKER password recovery software[48],, KRyLack Archive Password Recovery[49], *Advanced Archive Password Recovery etc* available in market for cracking password of various popular software programs or file types.

A criminal can deliberately hide data using some data hiding software or hardware techniques [50]. Hardware based method hide data in specific area of storage media such as HPA (host protected area), DCO(device configuration overlays), UPA(un-used partitioned area) and inter partition. The software based data hiding methods may use slack (file, volume and partition) space for hiding data. Bmap (Linux), Slacker (Windows NTFS) data hiding tool, can utilize slack space in blocks to hide data. The forensic experts recover such hidden data using some data recovery services.

Steganography is an art and science of writing hidden messages. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol[60]. The stenographic softwares hide a file within a file. QuickStego, OpenStego, OpenPuff, Virtual Stenographic Laboratory (VSL) etc software can hide text data in image file. These hidden information can be recovered using anti-stenographic software such as: AntiSteg 2.00, Stego (**Hunter**, Watch, **Analyst, Break)[51],** StegDetect[52], Stegnography studio[53] etc.

The various tools mentioned in subsection *IV* (*A-B*) runs under different platforms. More over some tools are open source where as other are commercial. The user may choose best possible tool as per their requirement. A large variety of tools are available and we have quoted only some tools. The performance of these tools in comparison to each other needs to be further investigated.

If criminal is unaware about various possible locations of data stored by OS or application program then the chances of destroying evidences are less. On the other hand if the criminal is well aware about possible locations of digital records stored on memory device then he/she can play safe but this is possible only if your device is not on network. The various such files are: web cache, temp file, history of URL links, swap file, page files, web history, and application logs. If your device is on network then there are many intermediate device/computers that record your communication and destroying evidence on your computer means not it has been deleted from various intermediate computers\servers. Sometimes a data may be present in recycle bin which a crime perpetrator forgot to empty in haste or due to computer illiteracy.

7. DIGITAL SIGNATURE FACTS

The authenticity and integrity of a document can be validated using some mathematical techniques. The digital signature is a way of authenticating a message, mail or document much like a signature on a paper. Digital signatures are authentic, un-forgeable, not reusable, unalterable and non-repudiated. Both encryption and digital signature can be combined, hence providing privacy and authentication [54]. Digital Signature Algorithm (DSA) was adopted as FIPS 186 in 1993 first time as Digital Signature Standard (DSS). Its latest release is 186-4 2013 [55] and it is based on three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir Adelman Algorithm (RSA).

The electronic documents are required to be signed digitally using a Digital Signature Certificate to maintain its authenticity. A licensed Certifying Authority (CA) is granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000 and issues the digital signature. At present some organisations are authorized Certifying Authorities under Controller of Certifying Authorities (CCA), Government of India [56,59].

In India, the Ministry of Corporate Affairs has introduced the MCA21 e-Governance programme with a view to providing all services relating to Registrar of Companies (ROC) offices on-line in e-Governance mode. All filings from September 16, 2006 can be done only under the Digital Signatures of the authorized person [57]. Under MCA21 program two kinds of Digital Signature Certificates are valid[58] - Class 2: Here, the identity of a person is verified against a trusted, pre-verified database. Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

8. CONCLUSION

The advancement of technology has given birth to the crimes that pertain to the use of digital computer and its associated devices. The digital evidences generated using such devices are admissible as evidence in court. But the criminal can play with such evidence to escape themselves from the law. Such evidences can be deleted, destroyed and concealed using software tools. At the same time large number of software utilities have been developed to collect, recover such evidences from the digital devices. Indian courts are also admitting technological evidences particularly the digital evidences to pronounce their verdict. There is dire need of giving due care to collect, preserve and analyze them to avoid their misuse.

REFERENCES

[1] Information Technology Act, 2000.

[2] Section 2&5 of Information Technology Act, 2000.

[3] Section 2(*r & t*) of Information Technology Act, 2000.

[4] Section 2(*p*) of Information Technology Act, 2000.

[5] Section 2(*ha*) of Information Technology (Amendment) Act, 2008.

[6] Section 69 of Information Technology Amendment Act, 2008.

[7] Information Technology (Amendment) Act, 2008.

[8] http://indiankanoon.org/doc/187283766/

[9] Chris Hale, Cybercrime: Facts & Figures Concerning This Global Dilemma, Crime & Justice International Volume:18 Issue:65 Dated: September 2002, 09/2002.

[10] C. Easttom, J. Taylor Det, Computer Crime, Investigation, and the Law, Course Technology PTR, 2010.

[11] D. L. Shinder, Cybercrime Scene of the Computer Forensics Handbook, Syngress Publishing, Inc, 2002.

[12] Eoghan Casey, Handbook of Digital Forensics and Investigation, Elsevier Inc., 2010.

[13] http://eraser.heidi.ie/

[14] http://support.itmate.co.uk/?mode =Products &p= index.datsuite

[15] http://www.acelogix.com/ (Ace Utilities)

[16] https://www.piriform.com/ (CCleaner)

[17] http://ospc-privacy-cleaner.software.informer.com/ (OSPC: Privacy Cleaner)

[18] http://browsertools.net/IE-Privacy-Keeper/

[19] http://www.systenance.com/indexdat.php (index.dat Analyzer.)

[20] Privacy Mantra

[21] http://www.cmcm.com/en-us/clean-master/

[22] http://www.forensics-intl.com/safeback.html

[23] http://www.snapback.com /

[24] http : // www.digitalintelligence.com /software / guidancesoftware / encase /

[25] http://www.techpathways.com/prodiscoverdft.htm

[26] http:/ /accessdata.com/ products/ forensic-investigation/ ftk

[27] http://www.e-fense.com/helix3pro.php

[28] http://www.ilook-forensics.org/

[29] http://www.dibsforensics.com/raid%20_rapid.html

[30] http://www.x-ways.net/forensics/

[31] http://www.asrdata.com/forensic-software/smart-for-linux/smart-acquisition/

[32] https://www.paraben.com/forensic-replicator.html

[33] http://dcfldd.sourceforge.net/

[34] http://www.deftlinux.net/package-list/

[35] http://forensicswiki.org/wiki/DEFT_Linux

[36] http://www.caine-live.net/

[37] http://dmitrybrant.com/diskdigger

[38] http://www.easeus.com/data-recovery-software/

[39] http://www.handyrecovery.com/

[40] http://www.undelete-plus.com

[41] http://www.sleuthkit.org/sleuthkit/desc.php

[42] http://www.paraben-forensics.com/

[43] http: // accessdata.com/ product-download/ digital-forensics/ distributed-network-attack-dna-version-7.3.0

[44] http://ophcrack.sourceforge.net/

[45] http://www.l0phtcrack.com/

[46] http://www.oxid.it/cain.html

[47] http: // www.tenorshare.com/ products/ data-recovery-pro.html

[48] https://apasscracker.com/products/

[49] http://www.krylack.com/archive-password-recovery/

[50] Y. Guo and J. Slay, Data Recovery Function Testing for Digital Forensic Tools, Advances in Digital Forensics VI: proceedings of Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Springer; 2010 edition.

[51] http://www.wetstonetech.com/cgi-bin/shop.cgi?view,1

[52] http://www.apponic.com/publisher/niels-provos/

[53] http://www.stegstudio.sourceforge.net/

[54] http: // www.cgi.com /files /white-papers /cgi_whpr_35_pki_e.pdf

[55] http://nvlpubs.nist.gov /nistpubs/FIPS /NIST.FIPS.186-4.pdf

[56] http://www.cca.gov.in/cca/

[57] http://www.mca.gov.in/MCA21/dca/efiling/efiling.html

[58] http://www.mca.gov.in/MinistryV2/faq_DSC.html

[59] http: //wbcomtax.nic.in /e-Services /Certifying_Authrities.pdf

[60] https://en.wikipedia.org/wiki/Steganography.