A Review: Assessment of Indian Digital Defense & Forensics Investigation System

R. K. Prajapati, Rakesh Kumar Rai

Abstract: Computer forensic is a branch of science that does analysis of events happened in digital environment. Every change is traceable in digital form just like physical & chemical form of a material. Now technologies are rapidly growing to make convenient for everybody life. As we know science develops killing materials for us. This only provides some means like data processing, data storing, querying etc to solve our daily hard problems. Once events happened in digital environment will leave the trace or not? If answer is no then what we are developing really become a killing materials nothing more than that. But it is not always true. Every change leaves a trace. These trace should be measured to identify and quantification of changes in digital environment. Today text, image, audio, video and animation various type of data are becoming common to share in digital communication. We all are very use to share our own pictures, videos online with our friends. But if something were changed by any person intentionally or unintentionally then it creates problems for us. In this paper we will discuss important digital documents that can be forged, available forging methods, tracing forgery in digital documents [8], [10], impacts on overall evidences and justice. Our main objective to discus some points in this paper that can be treated as milestones to seize & restore evidences to provide secondary opinion for honorable judiciary.

Index Terms---Forensics, Digital data, electronic evidence, steganography, volatile data etc.

I. INTRODUCTION

Computer forensic is known as branch of forensic science. So it will suppose to satisfy all basic principles of science. We have to deduce those basic principles in terms of digital form. Each and every things are measurable directly or indirectly in science similarly computer forensic is able to measure all changes.

DIGITAL forensics detects and observes abnormal conditions in digital applications or devices, including computers, PDAs, and networks, to determine the evidence [3]. In particular, Healy has extensively studied the feasibility of applying E-forensics in information science to digital devices such as mobile phones [4]. Hung-Min Sun et al have discussed various forensic related problems in their work [2].

II. FORENSIC CONTENTS & REVIEW

Investigating a single computer or laptop involved in an incident requires booting the machine into forensic mode and avoiding making changes in data or timestamps while doing the investigation is in progress. It cover data-hiding techniques and methods for recovering deleted files [2], the use of hash functions to identify files, and how to capture network packets and analyze traffic.

Manuscript received October, 2013.
R. K. Prajapati, I.T.S Engineering College, Greater Noida, India.
Rakesh Kumar Rai, I.T.S Engineering College, Greater Noida, India.

Today's forensic investigators working on behalf of law enforcement rarely archive images from multiple investigations on a single file server. Some practitioners have argued that it is important to work on one drive at a time to avoid the inadvertent mixing of information between cases. We believe that this argument is incorrect and that it emerges from an incorrect understanding of the Federal Rules of Evidence Article 10 (US Congress, 2004), sometimes called the ''best evidence rule'' [1].

III. ELECTRONIC EVIDENCES

It is required that information as an evidence should be authentic, reliable, and admissible by judiciary. Different countries have specific course of action and practices for evidence upturn. In the United Kingdom, examiners often go behind police investigating guidelines that guarantee the accuracy and truth of evidence. While voluntary, the guidelines are widely accepted in courts in Wales, England, and Scotland. E-forensics investigates and extracts confidential information from electronic products [2]. IntelliDact can automatically scan electronic documents and even handwritten notes (once digitized) for private information such as social security numbers, bank account numbers, drives license numbers, and credit card numbers [5].

IV. COMPUTER FORENSIC PROCESS

Computer forensic investigations usually follow the standard digital forensic process (acquisition, analysis and reporting). Investigations were performed on static data (seized digital data) rather than "live" systems. But due to technological development in advance forensic investigation practices there is no any slackness of techno-geek person, tools, and techniques. The computer forensic processes are different between cases to case, but the basic procedures are similar in all cases.

1. Seize the suspected media first. Capture in all respect so that no one can manipulate or divert investigation any way.
2. A bit-by-bit image/shadow is created from the suspected media, duplicate number of copies for making ensure that uncorrupted and unaltered copy is used for the investigation purpose.
3. Copy of one digital forensic image is now analyzed for potential evidence specific to each case. Deleted files, changed files, date & time stamp of media files, internet history, Instant messaging logs, system log file, emails, etc are all searched for analysis.
4. Evidence is extracted and prepared enlist for presentation in a legal form so that court can prosecute case in court. And these evidences can be treated as helpful item for secondary opinion of judiciary.
5. Finally investigator will create a customized report detailing the whole chain of events by findings in

process. Correlate all available events technically to each others for making the best decisions.

6. If it is required at any stage expert observer testimony is provided if needed in whole process to optimize the outcomes at any stage in whole process.

V. TYPES OF FORENSIC PROCESSES

A. Cross-drive analysis

A forensic technique that correlates information found on multiple drives. Extracted features can be used to speed initial analysis and answer septic questions about a drive images. This have successfully used extracted features for drive image attribution and to build a tool that scans disks to report the likely existence of information that should have been destroyed under Fair and Accurate Credit Transactions Act (The fair and accurate credit transactions act of 2003) [5].

B. Live analysis

The examination of computers within the operating system using customized forensics & administrative tools to extract evidences like process list, memory used, variables accessed, log files, time &stamp etc. The practice is useful when investigation will have to find volatile & sensitive digital data before the computer is shut down.

C. Deleted files analysis

It is very common technique used in computer forensics is the recovery of deleted files. Everybody agree that deleted file will upturn some clues to proceed the investigation in right direction. So modern forensic software must have tools should be powerful for recovering, reading and correlating these deleted files.

D. Volatile data analysis

Forensic Analysis ToolKit (FATKit) – a modular, extensible framework that increases the practical applicability of volatile memory forensic analysis by freeing human analysts from the prohibitively-tedious aspects of low-level data extraction. FATKit allows analysts to focus on higher-level tasks by providing novel methods for automatically deriving digital object definitions from C source code, extracting those objects from memory images, and visualizing the underlying data in various ways. FATKit presently includes modules for general virtual address space reconstruction and visualization, as well as Linux- and Windows-specific kernel analysis [6].

E. Analysis through software tools

S. No.	Name	Platform	License	Version	Description
1.	BlackLight	Windows/Mac	Commercial	2013 R1.1	Windows, Mac and iOS forensics analysis software
2.	MacQuisition	Mac	Commercial	2013 R1.1	Mac data acquisition and imaging solution
3.	Spector CNE Investigator	Windows	commercial	7	A user activity monitoring solution that allows the replaying of computer activity in detail.
4.	Internet Evidence FinderIEF	Windows	commercial	5.5	Computer Forensics Solution

Table-1: Tools used for forensic investigation

F. Passive vs. Active Image Forensics

Digital image forensics is called passive if the forensic investigator cannot interfere with the image generation process and control type and/or appearance of identifying traces. The image generation process is considered as a 'read-only' procedure and the forensic investigator is confined to examine image characteristics that are generated by this process.

Identifying traces in passive image forensics in general divide into device characteristics (manufacturers use different components or adjust parameter settings for different devices, technological imperfections) and processing artifacts (traces that are introduced by post-processing). they are a means to assess image authenticity Active approaches differ from passive approaches in that the generation process is purposely modified at an earlier stage to leave behind specific identifying traces. It establishes a link to the image's origin or ensures the image's authenticity. Consider for instance the embedding of a digital watermark, which is just an additional component to the overall image generation process, specifically conceived to produce identifying traces.

VI. COMPUTER FORENSIC IN INDIAN SCENARIOS

The laboratory is concentrating its efforts to update the technology and infrastructure by new state-of-the-art technology. The procurement of new technology for the division namely (1) Brain Finger printing (2) Voice Stress Analysis (3) Toxicology (4) Analog/Digital Audio/Video analysis is in process. Initiatives have been taken for a Quality management system, Technical up gradations, Calibration Systems, etc.

A proposal under 11th Five Year Plan has been mooted by the CFSL (CBI) to establish Scientific Aids Units (SAUs) in two metropolitan cities i.e. Kolkata and Mumbai and to strengthen the existing SAU at Chennai [9].

A. About central forensic science laboratory

The Central Forensic Science Laboratory, (CBI) New Delhi was established in the Year 1968 as a scientific department to provide scientific support and services to the investigation of crime. The Laboratory is located at Block No.4, CGO Complex, Lodhi Road, New Delhi-110003. Besides this, the CFSL has Scientific Aids Unit located at CBI Branch in Chennai. The Central Forensic Science Laboratory, CBI, New Delhi today is one of the most comprehensive Laboratories in the country with 10 fully equipped Divisions namely Physics, Chemistry, Biology, Serology, Ballistics, Documents, Finger Prints, Forensic Psychology, Photo, Computer Forensic Science & Scientific Aids divisions with addition of state-of-the-art laboratories for Computer Forensics and DNA profiling. The Central Forensic Science Laboratory (CBI), New Delhi is committed to deliver the quality work for all its functional disciplines and is an ISO/IEC 17025 Certified laboratory.

B. Jurisdiction

CFSL, CBI, New Delhi is a scientific department under the administrative control of CBI and overall control of the Ministry of Home Affairs with the Govt. of India. CFSL undertakes the scientific analysis of crime exhibits referred by CBI, Delhi Police, Judiciary and Vigilance Departments of Ministries & Undertakings & State/Central Govt. Departments. The experts of CFSL examine the exhibits

forwarded by the Investigating Agencies and render expert opinion and substantiate their opinions in the Court of Law through court testimony and evidence. Scientists/experts also impart training to the CBI Investigating Officers and to other trainees of Forensic Science. The laboratory also undertakes R & D work related to art & skill developments in forensic science [9].

C. MISSION OF CFSL

To provide assured quality service of international standards as per ISO/IEC 17025 to the customers with good professional practices in order to deduce effective remedial solution of intricacies related to Forensic Investigation of crime of any type and assist in proper dispensation of justice [9].

D. Facilities

The CFSL (CBI), New Delhi has the following divisions which are rendering forensic support services to the various Investigating Agencies in scientific analysis of exhibits and collection/detection of relevant physical clues from scenes of crime. The scientists of the laboratory are put to rigorous trainings in India and abroad in order to upgrade the existing forensic skills and to induct
innovative technologies in the field of Forensic Science like Ballistics & Explosives Division, Biology Division and DNA Profiling Unit, Chemistry Division, Computer Forensic Division, Document Division, Finger Print Division, Forensic Psychology Division, Physics Division, Photo & Scientific Aid Division, Serology Division and, Scientific Aid Unit of CFSL at Chennai [9].

E. Computer Forensic Division

Computer Forensic Division started functioning since January 2004. Its main objectives are preservation, identification, extraction and documentation of computer evidence in various Computer related crimes forwarded to the laboratory. Computer Forensics involves the use of sophisticated technology, tools and procedures. The accuracy of evidence processing procedures is ensured by using multiple software hardware tools developed by separate and independent developers. Validation through the use of multiple software tools and procedures by the computer experts eliminate the potential problem.

There are four central forensic laboratories in India, at Hyderabad, Kolkata, Chandigarh and New Delhi. CFSL Hyderabad is centre of excellence in chemical sciences, CFSL Kolkata (oldest laboratory in India) in biological sciences and CFSL Chandigarh in physical sciences. These laboratories are under the control of the Directorate of Forensic Science (DFS) of the Ministry of Home Affairs. The laboratory in New Delhi is under the control of the Central Bureau of Investigation and investigates cases on its behalf [9].

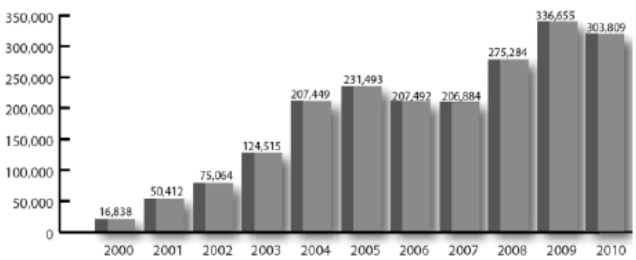

Figure-1: Yearly Comparison of Complaints Received Via the IC3 Website

Figure-2: Rise in registration of cyber crime cases in India (National Crime Records Bureau)

These figures (1, 2) show importance of this field in future. Things are being complicated due to virtualization of computing environment. But nobody will compromise their safety wearing all advance digital services & devices. If number of crime increasing such a way then manual handling and prosecution will always harsh. So digital forensic will help to find evidences from various sources and unhide a superfast links between incidences to correlate whole consequences.

VII. CONCLUSION

In many fields especially in image forensics when more than two images are joined as one to produce better quality image. It always does some arithmetic & geometric transformations such as scaling, rotations skew, clipping and manipulation in original images are desirable. Various operation required in image processing like geometric transformations require re-sampling and interpolation to change the original image in new one. So by using sophisticated re-sampling & interpolation detecting method /software tools all manipulated portion of an image can be identified. This will be solid tracing evidence to investigate related cases.

As discussed in various paper about importance of sophisticated method to deal such modifications but there are few published concept in this area of concern. Finally computer forensic is very extensive world today so packages of software tool should be developed that can compete all possible forgeries related to computer. As technologies grow detection of changes & degree of changes in digital form will always a challenge for researchers. Investigation planning is very important role in throughout Forensic investigation process. Second important activity is evidence acquisition & analysis. Finally step is reporting all those findings for presentation in a legal form. Evidence acquisition and analysis require specialized software tool to segregate digital data from various source. Collected data will exhaustively analyze to deduce the logical conclusion. So there is thrust of such specialized tools & techniques.

REFERENCES

[1] Matt Bishop, Deborah A. Frincke, " Teaching Digital Forensics to Undergraduate Students" IEEE Security & Privacy, May/June 2008, page 54-56.

[2] [2]Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, and Cheng-Hsing Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 7, AUGUST 2011, p1392-1403.

[3] V. M. Potdar, M. A. Khan, E. Chang, M. Ulieru and P. R. Worthington, "E-Forensics Steganography

System for Secret Information Retrieval," Advanced Engineering Informatics, vol. 19, no. 3, pp. pp. 235-241, 2005.
[4] R. Healy, "Using Electronic Evidence form Proprietary Devices: Opportunities and Implications for Court Evidence," in Proc. Seventeen International Symposium forensic sciences, New Zealand, 2004.
[5] Simson L.," Forensic feature extraction and cross-drive analysis" , Garfinkel Center for Research on Computation and Society , Harvard University, Cambridge, MA 02139, USA.
[6] Nick L. Petroni Jr.a AAron Waltersb,Timothy Frasera, William A. Arbaugha, " FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory Digital Investigation", Volume 3, Issue 4, December 2006, Pages 197–210.
[7] Vidya Rajarao et al, "Safeguarding organizations in India against Cyber crime", PwC Brand and Communications India, Global economic crime survey 2011.
[8] Matthew C. Stamm and K. J. Ray Liu, "FORENSIC ESTIMATION AND RECONSTRUCTION OF A CONTRAST ENHANCEMENT MAPPING", ICASSP 2010, page 1698-1701.
[9] http://cbi.nic.in/cfsl
[10] Hany Farid ,"Image Forgery Detection", IEEE SIGNAL PROCESSING MAGAZINE, MARCH 2009, page-16-25