An Insight View of Digital Forensics

Neha Kishore, Chetna Gupta and Dhvani Dawar

Department of Computer Science Engineering, Chitkara University, Himachal Pradesh

ABSTRACT

Crime and violence are inherent in our political and social system. With the moving pace of technology, the popularity of internet grows continuously, with not only changing our views of life, but also changing the way crime takes place all over the world. We need a technology that can be used to bring justice to those who are responsible for conducting attacks on computer systems across the globe. In this paper, we present various measures being taken in order to control and deal with the crime related to digital devices. This paper gives an insight of Digital Forensics and current situation of India in handling such type of crimes.

KEYWORDS

Digital Forensics, Cyber Forensics, Computer Crimes, Fraud

1.INTRODUCTION

Today in the computers world, along with the computers, its users are also increasing very rapidly. Now the time has come in which organizations are strongly dependent on the computers and internet for taking their business to the crest. A large package of information is being sent or received at one click. The large numbers of computers are connected in a cob-web like network, which is necessary for dispatching and receiving information. Along with boom, these computers are also responsible for Cyber Frauds and Cyber Crimes (CFCC).

In simple words, Digital Forensics [1] is a branch of forensic science related to the use of digital information produced, stored and transmitted on computers as source of evidence in investigations and forensics. Digital forensics exists from as long as computers have stored data that could be used as evidence. It has recently gained significant popularity with Government and many local law Enforcement agencies.

The computer system and networks may not be used in execution of the computer crimes, but it form as a part of the computer crimes. Digital forensic analysis of these types of system and networks can provide digital evidences e.g., planning a murder, cyber harassment, pornography, theft of electronically stored information and data generate fraudulent documents with the help of scanners and printers. So the role of Digital investigation in solving the case can lead to a complete change in the investigation if the same is done properly[2].

Internet is most important application for modern society persons. Internet has a lot of convenience to communication between human races all over the world. Due to rapid developments and lack of proper rules and regulations, it has become a crime hub.

In the rest of the paper, we have given an overview to digital forensics and its shortcomings. In section 2, we deal with digital forensics which is a technical aspect for investigating crime cases

DOI:10.5121/ijcsa.2014.4608

with its categories and abstract model. Latter in section 3, ethics and cardinal rules to be followed while producing proof in the court of law along with the tools used have been discussed and in Section 4, some recent cases of cybercrime happened in India have been covered. Section 5 covers future scope which will help to minimize crime by introducing new models followed by conclusion and references in section 6.

2.DIGITAL FORENSICS

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime [3],[4]. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.[3] With roots in the personal computing revolution of the late 1970s and early '80s, the discipline evolved in a haphazard manner during the 1990s, and it was not there by early 21st century that national policies emerged.

Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.

2.1. Classes of Digital Forensics

Digital Forensics can be categorized into following types which helps the agency to proceed to investigation according to the genres defined.

- *Device Forensics:* This trade deals with mindboggling digital devices which are used for storing data of personal and professional nature, devices such as PDA, mobile phones, digital cameras, scanners and many more. By using variety of tools relevant data need to be unearthed.
- *Disk Forensics:* In this branch the data is extracted whether it is erased, appended or presently stored on any storage medium such as Floppy, Hard Disc, CD, Flash Drive, USB Devices etc. in order to gather information from it.
- *Network Forensics:* The digital world at its pace becoming interconnected by, the danger of losing digital data is imminent, information flows at click seconds through proxy servers, and several network devices which have global footprint making it hard for the investigation agencies to get full support from various unknown governments, authorities and agencies .Its mostly used for tracking industrial espionage, defamation cases, software piracy& data theft[5].

Based on these genres, we have come up with a model which helps to segregate the case into different modules. The model has been described in Section 2.2.

2.2.Digital Forensics Model

Different countries have their own set of rules and laws based on which they investigate crime cases. These laws lead to the formation of investigation models. So there is no standard model to perform Digital Forensics. We here present an abstract model of Digital Forensics in Figure1, according to the study and requirements.

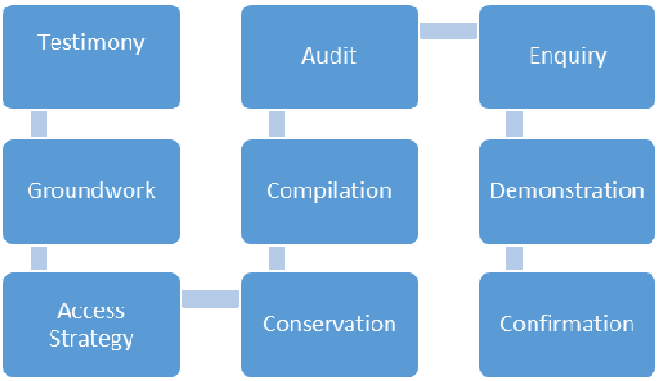

Figure 1: Digital Forensics Model

This model comprises of nine components for complete investigation:

1. **Testimony:** To recognize the type of incidents from indicators. It has influence on other steps or phases of this model.
2. **Ground Work:** To entail the preparation of search warrants and monitoring authorizations and management support.
3. **Access Strategy:** To develop a procedure to maximize the collection of evidences while minimizing the impact to the victim.
4. **Conservation:** To secure the state of physical evidences.
5. **Compilation:** To use standardized procedure to record the physical scene.
6. **Audit:** To entail an in-depth search of evidence related to the suspected crime.
7. **Enquiry:** To inspect the importance of examined product.
8. **Demonstration:** To explain all the phases involved.
9. **Confirmation:** Returning the digital evidences back to the owner [6].

In general, based on these components, the case is investigated performing each phase in order to deal with a case. Now further we discuss about various sectors which describes about the value of Digital Forensics.

2.2.Importance of Digital Forensics

The field of digital forensics has become increasingly more important over the last few years as both the computer and the cellular market has grown. Although there are probably hundreds of cases where Digital forensics can be used but we have segregated its use in three important sectors each having the most important aspects:

1. The Government Sector, the lawsuit includes Paedophiliac Rings Tracking, Unauthorized entry in defence networks, Homicide investigations.
2. In Corporate Sector, cases which are investigated are Theft of trade secrets, Software Piracy, Insider trading, Copy right, Embezzlement.
3. The type of cases included in Personal Matters are unauthorized use and Cyber stalking [5].

Digital Forensics has become an indispensable part of crime and law, no sector is left behind in this. Every country is taking special measures to deal with these type of crimes.

3.ETHICS TO BE FOLLOWED BY DIGITAL FORENSICS EXPERT

Digital Forensic expert is an investigator that investigates the digital evidences. The task of Digital Investigator is very crucial as any information left can lead the case in a different situation. So some ethics are expected to be followed by the Digital Investigator while conducting the investigation such as:

- The investigator shouldn't delete or alter any evidence, i.e., any proof related to the case should be kept at secure place and shouldn't be damaged.
- Should protect the computer/digital devices against viruses viz-a-viz viruses should be removed so that they don't destroy any information.
- Keep a log of all work done.
- Keep any Client Attorney information that is gained confidential [5].

The role of Digital Investigator in a Forensic investigation of a crime is complicated which starts at the crime scene, continues in to the computer labs for deep investigation, and ends in the court where the final judgment is done. There is no scope of negligence at all.

3.1Cardinal Rules to be followed while producing Evidence in The Court Of Law

Once the investigation is completed, the digital investigator also needs to ensure the rules provided by court in order to present the evidence. It should ensure:

a) *Authenticity* - Does the evidence being shown is actually authentic in the source from where it is extracted.

b) *Reliability* - Is the evidence being shown is true and can only be the source to rely on it. Forensic Computing is the specialist process of imaging [7] and processing computer data which is reliable enough to be used as evidence in court [8].

c) *Completeness* - Is the evidence complete in nature without any ambiguity to be produced in the court of law.

d) *Conformity with common law and legislative rules* –Is the evidence shown free from interference and contamination as a result of forensic investigation and other post-event handling.

e) *Check-lists* - supporting each methodology should be provided in case the evidence is challenged.

f) *Establish evidence custodian* - start a detailed journal with the date and time and date/information discovered.

Even after following these rules, not only digital crime cases but mobile, social media sites, cybercrime disputes occur in India and are unsolvable/traceable.

3.2 Tools in Digital Forensics

All digital evidences must be analyzed to determine the type of information that is stored upon it. Special tools are used that can display information in a format that is useful to Digital Investigators. Such Forensic Tools include FTK, EnCase [9], SMART, PyFlag and The Sleuth Kit etc. The various performance features are described in Table1.

Table 1: Digital Forensic Tools

Features	Encase	FTK	TSK
Language Interface	Traditional Chinese	Simple Chinese	English
User Interface	Must receive professional training	Ease of Use	Ease of Use
Create Image Profile	Support	Support	Support
Calculated of Hash Value	MD5	MD5	MD5 and SHA-1
Cost	Expensive	Expensive	Open Source Software
Advantage	Graphical Disk Information Interface	Classification of Digital Evidence	Support of many evidence, search techniques such as file data, keyword, metadata etc.

Depending upon the requirement and availability these tools are being used.

3.DIGITAL FORENSICS IN INDIA

India as a developing country and is still struggling hard with its security system. The rules and the laws related to Digital Crime are not that strong as that of the use of Digital Devices. Digital forensics and Indian approach have always been indifferent. Due to lack of manpower to manage the ever growing cases of cybercrimes, white collar crimes and corporate frauds, there are very few digital forensics institutions in India. The ones which are existing are heavily overburdened.

After seeing the exponential increase in Digital Crimes, the Indian government is formulating cyber forensics practices in India with assistance from private industries as the law enforcement agencies are still struggling to gain cyber forensics expertise.

In current scenario, techniques like IP address tracking and media forensics is not an important part of the investigation procedure of law enforcement agencies in India. For instance, lack of use of cyber forensics best practices in IPL match fixing case may jeopardize it. Similarly, forensics analysis of Nokia's computer used to download software in India has also not been undertaken properly.

The latest to add to this list is the defective cyber forensics approach of Central Bureau of Investigation (CBI) in Aarushi Talwar's murder case. According to media sources, the defence counsel in the Aarushi Talwar's murder case had challenged the prosecution

version of CBI that Rajesh Talwar was awake on the night when crime took place and had used Internet connection at regular intervals[10].

A recent case of death of the young 17-year-old student due to cyber bullying might be an extreme case but cybercrimes are on the rise in Kolkata that a recent TCS study has claimed is addicted to Facebook — a high of 85% of teens have an account there[11].

With the increase in number of crimes, the government has sanctioned the proposal to declare cybercrime cell as a police station exclusively for investigating crime cases. 98% cybercrime cases registered across the country includes fake profile or hurting comments posted on social networking sites.

4.1 Digital Forensics – IT Act

To minimize these crimes, the cops register crime cases under the traditional IPC sections giving the IT act 2000, a pass. The cops still remain divided on invoking the stringent IT Act instead of the regular IPC sections. There are a number of positive developments, as well as many which dismay. Positively, they signal an attempt by the government to create a dynamic policy that is technology neutral. This is exemplified by its embracing the idea of electronic signatures as opposed to digital signatures. But more could have been done on this front (for instance, section 76 of the Act still talks of floppy disks). There have also been attempts to deal proactively with the many new challenges that the Internet poses. "The tendency to lodge cybercrime cases under IPC sections is justifiable only relating to evidence. Say for example, an SMS or an image send through cell phone devices are only covered under IT Act and not IPC. There are a lot of such evidences which are admissible in a court of law under IT Act only," said a retired CID Deputy SP, who headed the cyber cell.

Hacking is also considered as a part of IT Act and not IPC. Only 3 sections in IT Act deal with prosecution of criminal offenses by police. These are: computer source document, hacking and publishing abusive material in electronic form. Cases under IT Act are investigated only by the police inspectors. To investigate such cases, one would need 130 inspectors alone. In a state where 91 cops man a lakh of population, cybercrime complains are not only being lodged but investigated.

5.FUTURE SCOPE

Digital forensic is a type of maturing science. These are the few pointers for direction of future scope of research in this area:

a) Application of the new model in variety of cases and improvement in light of feedback.

b) Identification of new constraints in terms of technological advancement will require model to be updated with time.

Most of the digital forensic tools are commercial version, whose costs are high and are operated by professional forensic, so we mostly use open source forensic tools because they are easy to use and are less costly. The open source tools for forensic investigations which reduce the cost of tools as compare to commercials tools. Each forensic tool has its own limitations and constraints. The existing tools show little effort to recover the file when the disk is magnetically altered and/or physically damaged and/or overwritten, by the experienced culprits. Hence there is an

urgent need to enhance the automated tools with the above-discussed techniques to make the computer forensic analysis a full pledged and legally valid.

6. CONCLUSION

The aim of cyber forensic science is: "…to demonstrate how digital evidence can be used to reconstruct a crime or incident, identify suspects, apprehend the guilty, defend the innocent, and understand criminal motivations[12]. Digital forensics is a daunting task for the agencies, the criminal doesn't need to manipulate the data only from within the physical confines of the computer room but also from the wireless networks loaded with precious information extending beyond the offices to nearby area, networks can be eavesdropped, computers at any physical distance can be susceptible to unauthorized data entry and manipulation. According to Anthony et al. [13]it is no longer a matter of "if your wireless network will be attacked but when".

Anti-forensics software are yet another emerging challenge, the Locard's principle states that when a crime is committed, there is a cross-transfer of evidence between the scene and the perpetrator but criminals may use anti-forensic methods to work against the process or interfere with the evidence itself [14].

In 2005 Roger's [15] states that unfortunately, we cannot completely control these issues and we will never be able to completely prevent the corruption of evidence. The ongoing advancements in technology have produced a trend which has reduced the physical size and altered the internalized storage components of digital devices. It is essential for law enforcement to be aware of the potential devices present at a crime scene[16]. Governments need to develop special tools and software whose working and knowledge is only provided to government agencies and labs.

REFERENCES

[1] (15 June). Digital Forensics. Available: http://www.techopedia.com/definition/27805/digital- forensics
[2] M. Worring and R. Cucchiara, "Multimedia in forensics," in Proceedings of the 17th ACM international conference on Multimedia, 2009, pp. 1153-1154.
[3] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol. 1, pp. 1-12, 2002.
[4] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," International Journal of digital evidence, vol. 1, pp. 1-12, 2003.
[5] P. Y. S. B. D. C. A. U. Bansal, "Cyber Forensics-The art of Decoding the Binary Digits," International Journal of Emerging Technology and advanced engineering, vol. 2.
[6] R. Kaur and A. Kaur, "Digital forensics," International Journal of Computer Applications, vol. 50, pp. 5-9, 2012.
[7] N. Kishore and B. Kapoor, "An efficient parallel algorithm for hash computation in security and forensics applications," in Advance Computing Conference (IACC), 2014 IEEE International, 2014, pp. 873-877.
[8] M. Pollitt, "Computer forensics: An approach to evidence in cyberspace," in Proceedings of the National Information Systems Security Conference, 1995, pp. 487-491.
[9] L. Garber, "Encase: A case study in computer-forensic technology," IEEE Computer Magazine January, 2001.
[10] F. Karan, ed.
[11] N. R. Dwaipayan Ghosh, ed.
[12] E. Casey, Digital evidence and computer crime: forensic science, computers and the internet: Academic press, 2011.
[13] A. Reyes and J. Wiles, "Cybercrime and Digital Forensics," ed: Syngress, 2007.
[14] R. Saferstein, "Criminalistics: An introduction to forensic science," 2004.

[15] R. M., "Anti-forensics," ed, 2012.
[16] D. C. Harrill and R. P. Mislan, "A small scale digital device forensics ontology," Small Scale Digital Device Forensics Journal, vol. 1, p. 242, 2007.

Authors

Neha Kishore is an Assistant Professor at Chitkara School of Engineering and Technology, Chitkara University, India. She is pursuing her PhD in the field of Parallel Computing and Information Security. Her area of interests also include CUDA, OpenMP, J2EE, Java, SQL, C, C++, TOC. She has attended various National and International workshops and has many research papers in her credits.

Chetna Gupta is a student of B.E. CSE at Chitkara School of Engineering and Technology, Chitkara University, India. Her primary objective is to pursue graduate studies in computer science and engineering, leading to a career in research. Her area of interest includes cyber forensics, computer vision and data structures.

Dhvani Dawar is a student of B.E. CSE final year at Chitkara School of Engineering and Technology, Chitkara University, India. Her core area of interest includes programming, cyber forensics, data structures and network security.