A Study to Examine Cyber Forensic: Trends and Patterns in India

Ms. Shruti Verma*
Dr. Saurabh Mehta**

Abstract

Cyber forensics is a technique which is used to examine and analyze the computer system for some evidence which can be presented in the court of law as a proof to solve a cyber crime case and give the punishment to the criminal. India being the democratic nation finds difficult to strike a proper balance between the legal and the judicial system. Police and the law enforcement agencies still believe in the legacy system and are reluctant to follow the new suit. In this paper an attempt is made to show the current scenario of the cyber forensics in India, difficulties faced by the police dept and legal dept. This paper also briefs about the trends and patterns of the Indian cyber forensic.

Keywords: Cyber Crime, Cyber Forensic

Introduction

In India the field of cyber forensics is very new and fresh. People are not aware about the term cyber forensics and its use. Gradually the nation is getting digitized, with fast connecting networks, easy internet availability and acceptance of the user. Cyber crime is also nurturing under the umbrella of growing technology. And this develops the need of cyber forensics in the system. But unfortunately in India cyber forensics is not implemented to the optimum level. Cyber forensics is an art which is required to detect the hints, clues and evidences from the digital data about the cyber crime to show the proof in the court of law and help the judicial system to take correct and precise decision against the criminal and help the victim. Cyber forensics can also help in prevention of criminal activities. Unlike traditional crimes cyber crimes are very sophisticated and fast, at the same time it is difficult to find an evidence about the cyber crime as the digital evidences can be easily destroyed. So the job of cyber forensic is very crucial, finding out the digital evidence from the computer system confististicated. Indian legal system somehow fail to adopt the concept of cyber forensics and still follow the legacy pattern to solve the cyber crimes, this does not gives accurate evidences and projects unjust results in the court of law so the victim is given no justice and criminal is set free. The process of forensics is very slow in India because of various legal and judicial factors this delays the hearing of the case. There are so many cases still are pending and criminals are set free to commit few more crimes. We have adopted the idea and concept cyber space but we need to change our approach towards cyber forensics.

Trend in India

In India point of consideration is the legal and judicial systems and there working which seems to be out dated, with the advent of cyber crimes there exists a need to change the current policies and construct a new techno-legal framework to combat cyber crime with the use of latest forensic technologies. Crimes like facebook account hacking, and email spoofing is very common in India but due to poor law enforcement and weak legal implications the criminal is set free to commit another crime. The cyber crime conviction rate is very less in India, where as the cyber crimes have increased in India. It can be the fear to get

Ms. Shruti Verma*
Research Scholar at JJT University, Jhunjhunu
Assistant Professor at SPN Doshi Women's College affiliated to SNDT Women's University

Dr. Saurabh Mehta**
Associate Professor and Head of Dept. at Vidyalankar Institute of Technology affiliated to Mumbai University

into the legal proceedings or the disappointment with the quality of services provided Indian internet users do not prefer filing the case with the police, less than 50 % of cyber crime cases are registered with the police dept. this set the criminal free for another crime.

Cyber attacks in India are done by other countries like China, Pakistan, US, Nigeria, UAE, Brazil etc. Crimes like phishing, email frauds, credit/debit card frauds, identity theft, virus etc. are very common in India. Home minister Mr. Rajnath Singh has conveyed the need of having strong cyber law monitoring and stringent cyber security. This can be achieved only if there is proper infrastructure available with proper mindset.

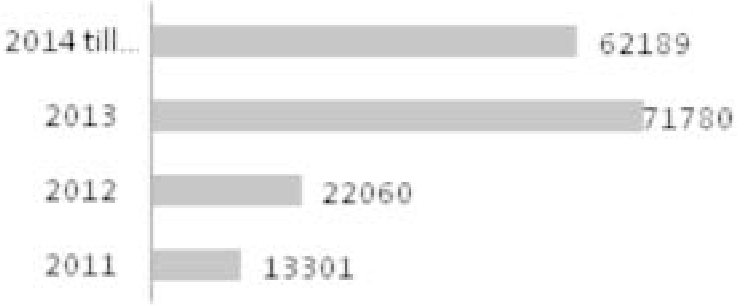

Figure 1. Total No. of Cyber Crime Reported [1]

The trends in this relation are not very good, above graph gives a clear picture of the drastic rise in cyber crime in last 4 years. Cyber crimes reported in the year 2011 are merely 13301 in contrast cyber crime reported in year 2014 till May is 62189 which might have touched the figure of 149254 approx. till the year end. It estimated that by 2015 cyber crime reported will be around 300000. [1][2]

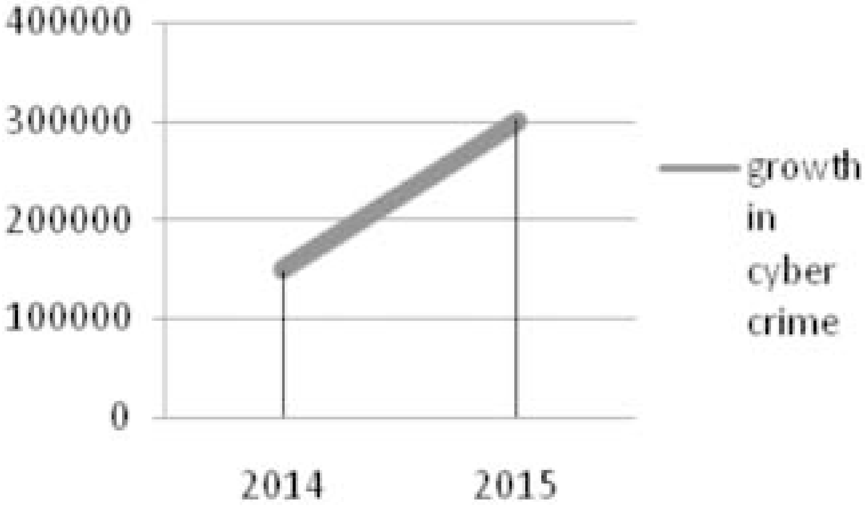

Figure 2. Sharp growth in Cyber Crime [2]

It is very much evident that increase in cyber crime will definitely raise the demand of forensics labs and implementation of cyber forensics in the investigation process. Forensics will find the evidence from the digital data at the optimum level and give accurate results; this will help the court to give proper judgment.

Cyber Forensics: A Process

i. As soon as the crime is reported and is registered with the police, investigation starts and data is collected from the place of crime / computer system and is examined using forensic techniques.

ii. The computer system seized is examined thoroughly to find out the digital data which can act as evidence.

iii. Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password protected files, log files, system files etc.

iv. After all the information is gathered from the computer system original form of evidence is recovered. It must very importantly kept in mind that never to harm the originally recovered data while applying forensics.

v. Create a mirror image of the original evidence using different mechanism like bit stream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for investigation.

vi. Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.

vii. Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

Packaging, Transportation and Storage [3]

Packaging is the process which is done after the computer system is seized at the crime spot. This computer system needs to be packaged properly so that no information is lost. Following steps must be taken care of –

i. Ensure that the electronic device seized is kept away from the magnetic field, static electricity as this may harm and erase the data inside the system.

ii. Computer system and the electronic devices seized during the investigation must be labeled, documented and numbered properly.

iii. Avoid bending or scratches on the electronic devices as this may corrupt the data stored.

iv. Pack the electronic devices in paper, paper box, and non static plastic bags.

Transportation is the process of carrying the digital evidence from the place of seizure to the place where something can be done about it (cyber forensic labs).

i. Care must be taken that the digital evidence are carried and transported with care over long distances.

ii. Extreme weather conditions like too much of heat, cold, moisture can harm the digital data, hence avoid prolonged storage of digital data.

iii. Avoid shocks and vibrations during transportation.

Data which is collected while investigation is required to be stored for some period of time till the court proceedings do not end. And ultimate care must be taken that this data is not tampered by any means in due course of time otherwise it may change the judgment completely.

i. Try to store the evidence in the secure place where it cannot be tampered purposely or incidentally.

ii. Storage place must be dry and with accurate weather conditions like appropriate heat, light, coolness and moisture.

iii. Batteries have limited life so always keep a note that prolonged storage can harm the important evidences like date, time etc. as if the battery gets weak and then is corrupt the system configuration may change the date and time settings.

Outlook of Cyber Forensics in India [4][5]–

The status of Cyber forensics in India can be viewed from three different angles which are equally important for the growth of the industry.

i. **Parliament –**

In India cyber forensics is still a developing field which is somehow getting less importance by our government.

As of now there are no rules and regulation drawn for cyber forensics this makes it difficult to collect the evidences.

The parliament are not very much interested in focusing on the techno-legal issues faced by cyber security, cyber forensics and cyber law.

There are many officials still unaware about the working of digital technology if these key officials of the country are reluctant towards the technology then its impact will be seen on the growth and development rate of the country.

ii. **Judicial system**

Judicial system are struggling in giving the judgments because of unstructured cyber law.

As the Indian cyber law consists of some loopholes it becomes difficult for the judiciary system to take a decision.

iii. **Police System**

As there are no standard procedures set up to collect the evidence and proceed with forensic.

The police have to face troubles and crisis, also the infrastructural limitation adds to the cause.

India is facing the problem of inadequate research and development infrastructure. The mindset of the people needs to be changed. Current status of Indian forensic labs is –

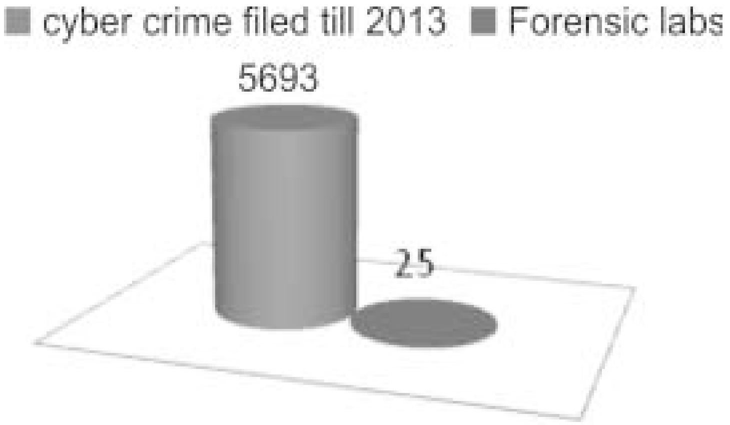

Figure 3. Cyber Crime v/s Forensics Lab [6]

From the above graph even if assume that every state is having at least one cyber forensic lab the ratio of the cyber crime committed and the forensic lab is very poor.

India needs to develop well equipped cyber forensics lab in every major police head quarters. The cyber forensic labs cannot get set up in one strike there has to be a step by step process which is time consuming. There is an absolute need of cyber forensic training institutes in India. There is a need to make policy and train the Police, Lawyers, Judges as well as common man. Education system of India should develop young once with the scientific and research mindset from the school levels.

India needs to concentrate on the development of the legal framework and structured procedures to solve the crime cases and complete the forensics in order to combat cyber crimes.

Suggestions and Recommendations

i. India needs to work in the direction of re framing and re constructing the cyber law.

ii. India needs to formulate the cyber forensics rules and regulation and must have a framework to regulate the policies.

iii. Immediate attention should be drawn towards creating awareness about the cyber forensics among the professionals and the police.

iv. Police Modernization and well equipped infrastructure.

v. Regulations and guidelines for effective investigations.

vi. Scientific approach towards digital data/ evidence.

vii. Research and development mindset should be maintained and inculcated among the young generations.

viii. Government should invest in the infra-structural arrangements for the training and lab equipments.

References

1. Cert-in reports over 62000 cyber attacks till May 2014 http://www.livemint.com/Politics/NNuFBA3F2iX4kxIXqKaX2K/CERTIn-reports-over-62000-cyber-attacks-till-May-2014.html
2. Cyber crimes likely to doubleto 3 lakhsin 2015 http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670_1_cyber-crimes-online-banking-pin-and-account-number
3. Rohas N., "Understanding Computer Forensics", Asian school of cyber law, 2009
4. International ICT Policies and Strategies http://ictps.blogspot.in/2011/06/cyber-forensics-laws-in-india.html
5. Cyber Forensics and Indian Approach http://ptlb.in/cfrci/?p=15
6. Indian Government Agency Received http://www.medianama.com/2014/12/223-cybercrime-india-2014/
7. Kazi M., Farooque G., Parab G., "Intellectual Property Rights & Cyber Laws", vipul prakashan, june 2013
8. Cyber Forensic Investigation Solutions in India Are Needed - http://ptlb.in/cfrci/?p=9
9. Cyber Forensics http://www.cyberlawsindia.net/computerforensics1.html