Analysis of Cybercrime Investigation Mechanism and Counsel of Defense in India

M. Elavarasi[1] & N. M. Elango[2]

[1]Research Scholar (Part-Time), Bharathiar University, Coimbatore - 641046, Tamil Nadu, India
[2]Associate Professor, School of Information Technology and Engineering, VIT University, Vellore - 632014, Tamil Nadu, India

Abstract: Cybercrime is an evolving crime when compare to other mode of crimes. It is rapidly increasing day by day. The law enforcement agencies in India should be more responsible in identifying this type of crimes. Cybercrimes are increasing but lack of cyber forensic experts to handle the crimes by using forensic tools. In India, we must increase the no of forensic experts and trained police officials and giving training for judicial officers.

Now a day's computers and other IT enabled devices are the tools for committing technical crimes by the criminals. The offences are listed as kidnapping, homicide, cheating, forgery and counterfeiting. Terrorist also using the gadgets like smart phones, tablet, IT enabled devices and encrypted pen drives for committing cybercrimes. In this paper, we are going to discuss about the investigation methodology followed by the police department and the counsel of defence in court in India.

Introduction

Computers are used as technology for enhancing the modern life in private, educational, commercial and government organisations. This will increase the productivity and efficiency of these entities. On the other hand, the use of technology is the root cause of the criminals for doing unlawful and unethical activities by using the computers.

Collection of evidences from the computers and IT enabled devices is a challenging job for the police and investigating agencies in India. investigation and collection of evidences from computers requires knowledge and computer skill is lacking in most personnel in our country. This leads to our government to go with agencies.

Steps Involved in Cybercrime Investigation

In this digital India lot of technology and many developments are taken place and many new inventions are still under process. With this increasing technology the crimes related to technology also increasing. Many cases are registered under IT act 2008 and it is get amended in 2010. Some of the cases registered are data theft, hacking, unauthorized access, pornography, intellectual property theft, cyber terrorism, viruses and many. cybercrime has become a large threat to the business, national security and for the common man. The following are the process of cybercrime investigation methodology

Questioning

Trying to collect the information about the crime, why it has done who committed and how to proceed the investigations.

Gathering Information

By checking web cameras, wire taps etc., sometimes the evidence also collected from the hacker's computers also.

Computer Forensics

After the process of questioning and information gathering the forensic tools are used to collect the evidences. The collected evidences are should be maintained carefully because it has to be produced in court.
Techniques of cybercrime investigation:

- Searching Who is
- Tracking IP address
- Analysis of web server logs
- Tracking of email account
- Trying to recover deleted evidences

- Trying to crack the password
- Trying to find out hidden data

A computer forensic investigator should follow some of the investigation methodologies in order to find out the truth. They have to follow some procedures to find out the truth. He should gather the evidences without affecting the chain of custody of the evidences. Once the evidence has gathered he should maintain the original data safely and he should work on the duplicate data. Data integrity should be maintained by the forensic investigator.

Forensic investigator should follow the following steps in investigating the cyber forensic cases. The process of investigation should not ruin the reputation of the investigator and also the reputation of the organization.

- For legal opinion the company should call for a legal advisor
- The first response of procedures (FRP) is prepared by the forensic investigator.
- The evidence from the crime scene are gathered by forensic investigator and it is afterwards taken to the forensic lab.
- The collected evidences are prepared as bit stream images and it is converted to MD5 hashing algorithm.
- Before concluding the investigation, the forensic investigator should examine the evidences and finally he should prepare the investigation report
- Finally, the forensic investigator should hand over the investigation report to the client.

Investigation of Cybercrimes Cases by Police Department

Emerging trends in cybercrimes which includes identity theft, hacking, phishing, spamming and cyber stalking. With these emerging types of crimes it is time for us to revamp and reform the investigation methodology which will be useful for prosecution of cyber crime cases. The police department is completely having lacuna in this field of investigation.

There are several potholes are existing in the system for investigation which includes the gap between the reporting of crimes, arresting the criminals and finally producing the criminals for prosecution in cybercrime cases.

According to the section 16of criminal procedure code and section 2 of Indian penal code will be used in handling the cases including territorial jurisdiction.

A legal and law manual has been framed to avoid the lack of operational manual which describes the methods of managing and doing on investigation related to cybercrimes. A standard investigation procedure has to be framed in order to investigate cybercrimes.

The cyber crime cells which are operating now should be equipped with highly technical staff and also they should have high technology crime and investigation infrastructure. In addition to the technical experts should also be recruited for cyber crime cell. The police are lack of experience and knowledge in handling cyber forensic tools like data transfer tools, password cracking tools etc. the forensic laboratories in district level also scared to handle the data's due to lack of technical skills.

Suggestions

There is a need to secure procedures connected with manpower for prosecution of computer-based crime cases to tackle them on a war footing. It must be secured of that the system provides for strict punishment of computer-crime and computer criminals so that the same acts as a method to prevent crime for others. Now, most of the offences committed under the Information Technology Act are Bailable with punishment up to 3 years imprisonment. This punishment should be increased to a term which would change the set of opinions of a computer-criminal of committing almost the same and like offences again. Separate bench is needed to be made up equal to for fast following and recording of Computer cases in an effective manner. With the constitution of cyber judges, the police department can prove the talent in cybercrimes cases.

References

1. www.tigweb.org/actiontools/projects/download/4926.doc
2. https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm
3. https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india
4. http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW
5. https://cybercrime.org.za/definition
6. http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws
7. https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf
8. http://searchsecurity.techtarget.com/definition/emailspoofing

9. http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html
10. http://ccasociety.com/what-is-irc-crime/
11. http://searchsecurity.techtarget.com/definition/denialof-service
12. http://niiconsulting.com/checkmate/2014/06/it-act2000-penalties-offences-with-case-studies/
13. http://www.cyberlawsindia.net/cyber-india.html
14. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
15. https://www.ijarcsse.com/docs/papers/Volume_5/8_ August2015/V5I8-0156.pdf