Research Paper Law

CYBER Forensics in Combating Cyber Crimes

Dr. Anjani Singh Tomar

Asst. professor of Law, GNLU, Atalika Avenue, Knowledge Corridor, Koba-Gandhinagar 382 007 (Gujarat) INDIA

ABSTRACT

The continuing technological revolution in communications and information exchange has created an entirely new form of crime: cyber crime or computer crime. Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. This is what has developed into the science of computer forensics. The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal. To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study. This paper analyze the role of cyber forensics in combating with cyber crimes& use of various emerging tools in the field.

KEYWORDS Cyber law, Cyber forensics, cyber frauds, computer crimes

INTRODUCTION:

"Forensics is the application of science to the legal process."

Jim Christy, DCCI

Computer crime and computer-supported criminal activities are booming businesses. Criminals, fraudsters, and terrorists seem to strike whenever there is an opportunity. Electronic evidence and information gathering have become central issues in an increasing number of conflicts and crimes which resulted into emergence of a new branch in forensic sciences i.e cyber forensics or computer forensics. It is about extracting evidence from computers that is sufficiently reliable to stand up in court and be convincing. Computer forensics is one of the largest growth professions of the twenty-first century. The term cyber forensics has many synonyms; it is also known as computer forensics. It is youngest branch of Forensic Science. Cyber laws particularly deal with the crime or legal issues related with internet. We find its origin in late 1980s where the practitioners used it to refer to the examination of standalone computers for digital evidence of crime.

Computer forensics or cyber forensics can be defined as "the collection and analysis of data from computer systems, networks, communication streams (wireless) and storage media in a manner that is admissible in a court of law". The amalgamation of the disciplines of computer science and the law result in cyber forensics. The anthology of information as well as the scrutiny of the basic embryonic data can be applied with this definition.

Traditionally Cyber forensics involves the:

- preservation,
- collection,
- validation,
- identification,
- analysis,
- interpretation,
- documentation and
- presentation

Of computer evidence stored on a computer

The process of collecting, preserving, analyzing, interpreting data and information from the computer storage by guaranteeing its accuracy and reliability is termed as cyber forensic. "Forensics means application of science to a legal process thus cyber forensic briefly means, bringing admissible digital evidence before the court. Electronic evidences can be easily broken and can be easily modified. Apart from these, criminals, cyber thieves, dishonest and sometimes even honest employees wipe, hide, cloak, disguise, encrypt and destroy the evidences from the storage media by using a variety of shareware, freeware and easily available utility programs. An international dependence on technology along with the increasing presence of Internet as a strategic resource and key requires corporate assets which are well protected and safeguarded. Whenever such assets come under the attack, or when they are misused, the security professionals must be able to collect electronic evidence of such attack or misuse and utilize those evidences to bring justice to those who misuse this technology.

Cyber forensics is both a science as well as an art. With the evolving technology and changing at such fast pace, the rules governing the application of cyber forensics to the fields of auditing, security, for defence and law enforcement are changing as well. New procedures and techniques are designed to give the professionals of info-security a better means of finding such electronic evidence, collecting the same, preserving it, and then presenting it to the client management for prospective use in the trial of cyber crimes.

The secrecy provided by Internet and the aptitude for society's criminal factors to access information technology as a means for financial and social discourses mandates the professionals who are charged with the liability of protecting and safeguarding critical communication resources have the tools to do so.

DEMAND FOR CYBER FORENSICS:

As computers have become more prevalent the concept of cybercrime has gained more awareness and threat in mind of the people since the criminal by sitting at one place can attack in any corner of the world or can commit a crime at any place. Hence, people specialized into the aspect of computer forensics are required to deal with the matter in a more prudent and reasonable manner. There is an increasingly need of computer forensics which should function accurately at all the level of the government and society. Where on one hand internet serves as a boon on the other hand it also opens the doors of the wrong doers for making ease the crime they are committing. People can access someone else's computer system without their authorization which results in issues related to security and privacy in the computer world. The computer forensics alerts the wrong doer for preventing the crime they are committing. It serves as a threat against those who carry out activities with a mala-fide intention and with a negative mind.

Cyber forensics has become vital in the corporate sector. There

are possibilities of theft of important data or information with respect to company's financial position which can be misused if gone in reprehensible hands. The organizations in such cases have to suffer heavy financial losses which may or may not be compensated at later stage. In such situations it is in the best interest of the company to hire the computer forensic specialists for the purpose of gathering information and evidence which can help in proving the suspect guilty of committing the crime.

It is also efficient wherein the information is stored in single system for the purpose of backup files. The intentional damage and data theft in a single system can be reduced by computer forensics. The hardware/software that employs the security measures for tracking the updating and changes of the information or data. The user information which has been provided in log files can effectively be used to generate the evidence if needed in any criminal or legal matter.

The main rationale behind computer forensic is to produce evidence before the court of law so that the court can punish the actual offender. Forensics is all about collecting the evidences in a scientific manner so that the utilization of the scientific knowledge is done in an appropriate manner for collecting information for supporting the actual fact.

The need for computer forensics is to make sure the honesty and reliability of the computer system. Computer forensics provides in depth the knowledge for understanding of the technical as well as legal aspects of computer related crime. It is very helpful in tracking down the cyber terrorism and upto a certain level can also be prevented from committing it. Computer forensics has also proved helpful in tracking down email spamming and child pornography issues and serves as a proof for the same.

The growing incidents of cybercrimes such as ransom ware, identity theft, and phishing have cost the country $4 billion during August, 2012-July, 2013, according to a report released by Internet security solutions provider Symantec.

The average cost per cybercrime victim in India grew 8 per cent to $207 during the period from $192 in the year-ago period, the 2013 Norton report adds.

The report, which is one of the largest global studies investigating the impact of cyber crime on consumers, is based on responses from 13,022 adults across 24 countries, including 1,000 from India.

If just look at the report in State of Orissa, the situation is worse,while only 27 cyber crime cases (both under IT Act and IPC) were registered in the state in 2012, it jumped to 104 in 2013. 12 cases were registered for 'tampering computer source document', three cases were reported for 'obscene publication and transmission'. Eleven cases were filed for making 'fraud digital signature' and 33 cases registered for alleged forgery, which came under IPC.

And other parts of India have witnessed same things in relation to cyber crimes.

TOOLS USED IN CYBER FORENSICS

With increase in serious issues like cyber terrorism, cyber stalking, spams, etc. cyber forensic tools aid in investigating such criminal cases and also for drafting and creating hard admissible evidences.

Some of such tools are as follows:

- **X-Ways WinHex:**

It is used as a low-level data processing, for inspecting files, for recovering digital camera card, for recovering the original file from the corrupt files systems, etc. This is a powerful tool used for gathering digital evidence.

- **First On Scene:**

FOS is a visual basic script code. It also works with other tools such as PSTools, LogonSessions, FPort, NTLast, PromiscDetect, FileHasher, etc. in order to create an evidence log report. This can be further analyzed by forensic experts for extracting important information.

- **Rifiuti:**

Rifiuti is a tool which helps in finding the last details of a system's recycle bin. It helps in collecting all the deleted and undeleted files.

- **Pasco:**

Pasco is a Latin word meaning "browse". Pasco helps in the analysis of the contents of what all browsing has been done from ones computer. In short it is particularly useful in gathering records of internet activities carried out from a targeted computer.

- **Galleta / Cookie:**

Galleta means "cookie". Galleta helps in examining the contents of cookie files on a computer. Cookie files are temporary internet files used by websites for maintaining their indigenous logs for purposes like tracking and etc.

- **Forensic Acquisition Utilities (FAU):**

It is a set of forensic tools such as checker; file wiper, etc. used for assorting research and investigation.

- **NMap:**

It is a port scanner tool that helps find open ports on a remote machine. NMap has an ability to evade source machine identity and works without causing any Intrusion Detection System (IDS) alarms to go off. It is mainly associated with the network security system.

- **Ethereal:**

Ethereal is another network security tool which is a network packet sniffer. it sniffs data packets over the network and provides incoming - outgoing data sent over the network, to the investigator. However, cannot be used in cases where strong encryption algorithms are placed at the source and destination computers.

- **BinText:**

BinText is useful to browse through gathered evidence files such as that of log files generated by other forensic tools. It is used for pattern matching and filtering these log files.

- **PyFlag Tools :**

PyFlag are a couple of tools used for log analysis and can be a very effective tool for investigators.

- **Encrypted disk detector :**

EDD is a command-line tool that quickly checks the local physical drives on a system for encrypted volumes. The decision can then be made to investigate further and determine whether a live acquisition needs to be made in order to secure and preserve the evidence that would otherwise be lost if the plug was pulled.

- **MemGator:**

Memgator is a memory file interrogation tool that automates the extraction of data from a memory file and compiles a report for the investigator. Data relating to memory details, processes, network connections, malware detection, and passwords and encryption keys can be extracted.

There is one another technique used for cyber forensic not particularly falling under the ambit of the tools used is, Miscellaneous Steganography Tools. It is basically a technique where data or a text file is converted and then embedded into an image file in order to deceive others. There are some tools however that help in detecting such injections. Hackers and malicious users are coming up with such ideas to inject data files into not just as image files but also as music and video files

At times individuals try to hide their incriminating informa-

tion by renaming a file of a particular type to another type by changing its extension. By doing so, it makes it difficult for one to determine the correct type of the file. In order to flag such suspicious file Encase is used; by running hash (#) functioning to the hard drive will interpret file headers and mark them as containing incorrect header information.

In order to make these information / evidence admissible in the court of law, it is very essential to create an exact image of the information. And for this the specialists work very hard, with all patients and accuracy , with all confidentiality that no one should know on what they are working on, and with all dedication in order to collect vital information which can be produces ad a concrete evidence before the court.

Once the information and all evidences are gathered, a compiled report is made by the specialists that can be produced before the courts. As these people are expertise and have special training regarding use of such complex tools and techniques they can also testify before the court regarding the matter they are working on.

Now a days, angry employees with malicious intention have assaulted many e-commerce website, such as viruses, wiretapping and financial frauds in various governmental of independent firms and companies. This e-commerce attaching causes various financial hardships to the companies. This has been observed as a common trait among the individuals who have been fired or have been insulted by the head departments, independent of hackers and such cyber criminals.

CHALLENGES FACED BY CYBER FORENSICS

No matter however effective any technology or system may be. There always has been a drawback to the same. Similarly, preserving data or information for the purpose of serving as an evidence is beneficial to the court but on the other hand there may be certain technical and human barriers to such gathering of the information. Some of the limitations are as follows:

- Some facilities which are there within the browsers for the purpose of saving the WWW pages to disk are not perfect because it may save the texts but not the related images
- There might be difference between what is there on the screen which can be seen and what is saved on the disk
- The method which has been used to save a particular file might not carry individual labeling regarding when and where it was obtained. Such files can be easily forged or modified
- Most times it becomes difficult for the system to locate the page which was acquired at last. If the entire series is examined it becomes even difficult to point which one was later and which was earlier.
- Many ISPs use proxy servers in order to speed up their delivery of pages which are popular on web. Hence, the user might not be sure of what he has received from that particular website by his ISP

Common mistakes like altering of the date and time stamps, killing of rouge processes, patching system before investigation etc lead to loose of data from the disk resulting in crashing of the e-files and evidences stored on the computer.

New technologies are helping the engineers to develop and create more robust hardware and software to investigate with respect to computer related crime.The advancement of encryption is one such challenge. If the encryption standard rise, so does the complexities in algorithms which makes it difficult for the specialist to decrypt a code and thus it becomes more time consuming. Another such challenge is maintaining credible certifications and industrial standards.

CONCLUSION

With the emergence of science and technology, cyber forensics has played a very important role. Moreover with the increase in the cyber crimes like hacking etc, the need of cyber forensics have felt , thus various tools and techniques have been developed for tracing the crime, making the exact report in order to make it admissible in the court of law. Various industries, corporations and governmental agencies now a days are keen towards appointing an expert in this field in order to check out cyber malfunctioning done by the employees. Such experts are appointed ti investigate the computer related crimes. After making an investigation, these specialist have to extract and prepare an exact repot of the evidence gathered through various mediums before the authority who asked him to do.

The existing forensic tools play a vital role in the aspect of the recovery. Each tool has its own constrains and limitations. There is need to make this tools and techniques more advance and enhanced to make computer forensics a full success and legally valid in law.

The future of computer forensics is limitless. With the expansion of technology the field will continue to expand along it its benefits and barriers. Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability. The evidence so collected by the specialist have to be handled and preserved in an appropriate manner, So that they can be produced before the court in its exact manner. Any process or methodology breakdown in implementation of the cyber forensics will ultimately lead to jeopardize of the case.

REFERENCES

• http://www.cyberlawsindia.net/computer-forensics.html | • http://www.webopedia.com/TERM/C/cyber_forensics.html | • http://computerforensicsinindia.blogspot.in/ | • http://www.ncfta.net/ | • http://en.wikipedia.org/wiki/Computer_forensics | • http://www.certconf.org/presentations/2006/files/WD4.pdf | • http://www.cyber-forensic-analysis.com/ | • https://my.infotex.com/wp-content/uploads/2012/03/computer_forensics_overview_isaca.pdf | • http://www.pinow.com/investigations/computer-forensics | • http://www.cyberforensics.in/(A(cos8NMWQywEkAAAAODMwODM4YWMtNWFmZC00ZWNhLThkNDEtNTlhMWM3MGE5MzA5hkCziwldj9ts_CCtkjYQl68akds1))/Research/DeviceForensics.aspx | • http://web.ics.purdue.edu/~pufsc/Cyber.html | • http://www.scribd.com/doc/15938005/Cyber-Crime-Investigation-and-Cyber-forensic | • http://computer-forensics.sans.org/blog/2012/09/07/digital-forensic-case-leads-anon-strikes-again-and-again-groupon-litigation-threats-darkmarket-motivations-revealed-the-tutu-has-been-donned | • http://www.articleswave.com/computer-articles/top-cyber-forensic-tools.html | • http://www.springerlink.com/content/wt84j6/front-matter.pdf | • http://www.cscjournals.org/csc/manuscript/Journals/IJS/volume3/Issue2/IJS-13.pdf | • http://www.theiia.org/intAuditor/itaudit/archives/2006/september/computer-forensics-a-valuable-audit-tool-1/ | • http://www.buzzle.com/articles/basic-cyber-forensics-and-techniques.html |