Page 786 - 798 **DOI:** *https://doij.org/10.10000/IJLMH.11543*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Role of Cyber Forensics in Investigation of Cyber Crimes

PRASHANT SAURABH[1] AND AMRIT JAY KUMAR ROY[2]

ABSTRACT

This research paper will describe cyber forensics, also known as computer forensics, which is a subdivision of digital forensic science, relating to evidence detection in computers and digital storage media. The purpose of cyber forensics is the forensically-sound investigation of digital media with the intent to: identify, preserve, recover, analyze, present facts, and opinions; concerning the digital information. Even though it is generally allied with the analysis of cyber-based crimes, computer forensics may also be used in civil proceedings. Evidence composed from cyber forensic analysis is typically subjected to similar procedures and performs as supplementary digital evidence. With these advancements, it was desired that cyber forensics be to protect users and remain citizen-centric. It also shows that there is additional research needed to understand the implications of cyber forensic research to improve detection of cyber-crimes.

Keywords: *Cyber Forensics, Digital Evidence, Forensically- sound investigation.*

I. INTRODUCTION

As Internet technologies proliferate into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted. The American Heritage Dictionary defines forensics as "relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law"[3].

Cyber forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and/or to rebuild the crime scenario[4]. According to computer forensics defined as the process of identifying, collecting, preserving, analyzing and presenting the computer-related evidence in a manner that is legally acceptable by court[5]. More recently,

[1] Author is a student at Patna Law College, Patna, India.
[2] Author is a student at Patna Law College, Patna, India.
[3] Kruse W.G, and Heiser J.G, Computer Forensics Incident Response Essentials, 2002, Addison Wesley Pearson Education, Boston
[4] Ibrahim M. Baggily, Richard Mislan, Marcus Rogers, Mobile Phone Forensics Tool Testing: A Database Driven Approach, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2
[5] Caloyannides, Michael A, Computer Forensics and Privacy. Artech House, Inc. 2001.

 [ISSN 2581-5369]

computer forensics branched into several overlapping areas, generating various terms[6] such as, digital forensics, data forensics, system forensics, network forensics, email forensics, cyber forensics, forensics analysis, enterprise forensics, proactive forensics etc.

Cyber forensics is the investigation of what happened and how. System forensics is performed on standalone machines. Network forensics involves the collection and analysis of network events in order to discover the sources of security attacks. The same process applied on Web is also known as Web forensics. Data forensics major focuses on analysis of volatile and non-volatile data. Proactive forensics is an ongoing forensics and there is an opportunity to actively, and regularly collect potential evidence in an ongoing basis. Email forensics deals with one or more e-mails as evidence in forensic investigation.

(A) Research methodology

1. Method of research

Pure doctrinal and analytical method of research will be followed. Various reports, articles, legal provisions and case laws will be used to study and prepare the present work. Primary as well as secondary sources of data will be used in this paper. Primary data includes various constitutions, legislations, judicial decisions of different nations and International conventions. The researchers will be using secondary sources of data such as books, various national and international journals, articles and materials available on the internet.

2. Research question

- Whether the acquiring of cyber forensics by the investigation officer amounts to the breach of right to privacy?
- Whether there are any established legal regimes for Cyber forensics among nations?
- Whether there is any possible solutions and suggestions for a better cyber forensics department in India?

3. Hypothesis

- The rules and laws made for cyber forensics and cyber security by the parliament, police system and judicial system in India and will help in finding loopholes in it
- The current trend and pattern of cyber forensics and cyber security in India so that cybercrimes can be prevented.

[6] Deepak Singh Tomar, Nikhil Kumar Singh, Bhopal Nath Roy, An approach to understand the end user behavior through log analysis, International Journal of Computer Applications (0975 – 8887) Volume 5– No.11, August 2010

 [ISSN 2581-5369]

4. Aims and objectives

- To study about the cyber forensics
- To know the rules and laws made for cyber forensics and cyber security by the parliament, police system and judicial system in India and finding loopholes in it.
- To know the current trend and pattern of digital forensics and cyber security in India

(B) History of Cyber Forensics

Until the late 1990s, what became known as Cyber forensics was commonly termed 'computer forensics. The first cyber forensic technicians were law enforcement officers who were also computer hobbyists. In the USA in 1984 work began in the FBI Computer Analysis and Response Team (CART). One year later, in the UK, the Metropolitan Police set up a computer crime unit under John Austen within what was then called the Fraud Squad.

A major change took place at the beginning of the 1990s. Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that cyber forensics (as with other fields) required standard techniques, protocols and procedures. Apart from informal guidelines, these formalisms did not exist but urgently needed to be developed. A series of conferences, initially convened by the Serious Fraud Office and the Inland Revenue, took place at the Police Staff College at Bram shill in 1994 and 1995, during which the modern British cyber forensic methodology was established.

(C) Overview of Cyber Forensics

Cyber forensics is used to help investigate cybercrime or identify direct evidence of a computer-assisted crime. The concept of cyber forensics dates back to late 1990s and early 2000s. The legal profession, law enforcement, policy makers, the business community, education, and government all have a vested interest in CF. Cyber forensics is often used in both criminal law and private investigation. It has been traditionally associated with criminal law. It requires rigorous standards to stand up to cross examination in court. It is becoming as a source of investigation because human expert witnesses are important since courts will not recognize software tools such as Encase, Pasco, and Ethereal as an expert witness[7]. Cyber forensics is useful for many professionals like military, private sector and industry, academia, and law. These areas have many needs including data protection, data acquisition, imaging, extraction, interrogation, normalization, analysis, and reporting. It is important for all professionals working in the emerging field of cyber forensics to have a working and

[7] Benjamin Turnbull, Jill Slay, Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection, IEEE Proceedings of the 40th Annual Hawaii International Conference on System Sciences-2007 (HICSS'07)

 [ISSN 2581-5369]

functioning lexicon of terms like bookmarks, cookies, web hit etc., that are uniformly applied throughout the profession and industry. Cyber forensics international guidelines, related key terms and tools are focused in the cyber forensics field manual[8].

The objective of Cyber forensics is to identify digital evidence for an investigation with the scientific method to draw conclusions. Examples of investigations that use cyber forensics include unlawful use of computers, child pornography, and cyber terrorism[9]. The area of cyber forensics has become prominent field of research because:

1. Forensics systems allow the administrator to diagnose errors
2. Intrusion detection systems are necessary in avoiding cyber crimes
3. Change detection can be possible with proactive forensics

(D) Cyber Crime

We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved[10].

Sussman and Heuston first proposed the term "Cyber Crime" in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts.[11] These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc. In simple term we can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems.[12] These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal[13]. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution. There is a myth

[8] Ashley Brinson, Abigail Robinson, Marcus Rogers, a cyber-forensics ontology: Creating a new approach to studying cyber forensics, Digital Instigation, Elsevier, 2006
[9] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012 Jun; 3(2):97-101.
[10] https://cybercrime.org.za/definition
[11] https://www.tutorialspoint.com/information_security_ cyber law/introduction.htm
[12] http://www.academia.edu/7781826/IMPACT_OF_SOCI AL_MEDIA_ON_SOCIETY_and_CYBER_LAW
[13] https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

among the people that cyber- crimes can only be committed over the cyberspace or the internet. New trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing[14] "botnet attacks"[15] and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP (VoIP) communication[16] and "cloud computing[17] It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

II. KINDS OF CYBER CRIME

Some major kinds of cyber-crimes are as follows:

(A) Illegal Access (Hacking, Cracking)

The offence which is described as "hacking "usually it refers to unlawful access to a computer system,[18] one of oldest computer-related crimes,[19] Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon.[20] hacking offences include breaking the password of password-protected websites[21] and circumventing password protection on a computer system.[22] But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally

[14] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions.

[15]Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4

[16]Simon/Slay, Voice over IP: Forensic Computing Implications, 2006

[17] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499

[18] In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

[19]See Levy, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf.

Taylor, Hacktivism: In Search of lost ethics? in Wall, Crime and the Internet, 2001, page 61; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.; Who is Calling your Computer Next? Hacker! Criminal Justice Journal, Vol. 8, 1985, page 89 et seq.; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777

[20]3 See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported; Biegel, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et seq. in the month of August 2007. Source: www.hackerwatch.org.

[21]Sieber, Council of Europe Organized Crime Report 2004, page 65.

[22] Musgrove, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

obtain a password to enter a computer system setting up "spoofing" websites to make users disclose their passwords[23] and installing hardware and software-based keylogging methods (e.g. "key loggers") that record every keystroke – and consequently any passwords used on the computer and/or device.

(B) Erotic or Pornographic Material (Excluding Child Pornography)

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping.[24]
- Worldwide[25] access, reaching a significantly larger number of customers than retail shops;
- The Internet is often viewed as an anonymous medium an aspect that consumers of pornography appreciate, in view of prevailing social opinions.
- Different countries criminalize erotic and pornographic material to different extents.[26] Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors[27] access this kind of material, seeking to protect minors. Studies indicate that child access to pornographic material could negatively influence their development. To comply with these laws, "adult verification systems" have been developed. Other countries criminalize any exchange of pornographic material even among adults,[28] without focusing on specific groups (such as minors).

(C) Child Pornography

The Internet is nowadays being highly used as a medium to sexually abuse the children. The children are viable and soft victim to the cybercrime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet as well. Pedophiles lure the children

[23] Supra note 26
[24] Depending on the availability of broadband access.
[25] http://cyber.law.harvard.edu/filtering/.
[26] One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch): Section 184 Dissemination of Pornographic Writings (1) Whoever, in relation to pornographic writings (Section 11 subsection (3)): 1. offers, gives or makes them accessible to a person under eighteen years of age; […]
[27] : www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[28] 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt): Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty

 [ISSN 2581-5369]

by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. They then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

(D) Cyber Stalking

In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victim's property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber stalking means repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services. Stalkers collect all personal information about the victim such as name, family background, telephone numbers etc. Stalker can be one of the acquaintances of the victim, or stranger to the victim. If he is victim's acquaintance, he can easily get this information. If he is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website and harass the victim through calls, emails etc.

(E) Steps Involved in Cybercrime Investigation

In the era of digital India, a 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 are also increasing. Many cases are registered under IT Act 2008 and also got amended in 2010. Some of the cases registered are data theft, hacking, unauthorized access, pornography, intellectual property theft, cyber terrorism, viruses and many. Cybercrime becomes a large threat to the business, national security and for the common man. The following are the process of cybercrime investigation methodology[29]

1. Questioning

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

[29] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012 Jun; 3(2):97-101.

precede the investigation.

2. Gathering Information

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

3. Computer Forensics

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

- Searching who is
- Tracking IP address
- Analysis of webserver 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. One should gather the evidences without affecting the chain of custody of the evidences. Once the evidence is gathered, one should maintain the original data safely and 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.

III. ROLE OF CYBER FORENSICS IN CYBER-CRIME INVESTIGATION

As cybercrime is increasing there is a robust need for cyber forensic experts in all industry models and more importantly among law enforcement agencies who rely on cyber forensics to find cyber criminals.

Cyber forensic investigators are the experts in investigating of the encrypted data using various types of software and tools. There are many upcoming techniques that investigators use depending on the type of cybercrime they are dealing with. The tasks for cyber investigators include recovering of the deleted files, cracking passwords, finding the source of the security breach etc. Once collected, the evidence is then stored and translated to make it presentable before the court of law or for police to further examine. The aim of cyber forensics is to

 [ISSN 2581-5369]

preserve evidence in its most original form so that a structured investigation can be performed to reconstruct past events.

IV. RIGHT TO PRIVACY IN CYBER FORENSICS AND CYBER SECURITY

When it comes to the development of Cyber- forensics in India, there is not even a single codified law which deals with this aspect of forensics. This can be due to the fact that technology law is still in its nascent stage in India. There are no regulations which are governing Cyber forensics, so if someone wants to become a cyber-forensic expert, he/she simply has to complete certified course on cyber forensics after finishing his graduation. There is no organization who governs the profession of cyber forensics in India. The primary use of cyber forensics in India is to deliver justice and solve the complicated cases, so it becomes very necessary to make a regulatory body which can check if the people in this profession are actually qualified enough to perform this task. Most of the time, the court of law has to rely on the data and evidences which are gathered from the investigation of digital media. This is due to the fact that most of the people now have access to internet which is also increasing the number of crime involving digital media. For example, if a girl is getting blackmailed on a messenger app, then the sole and most effective way of proving it in the court will be to give evidence, which in such cases, most of the time are in digital forms.

Right to privacy is a fundamental right which is guaranteed under the Article 19 of constitution of India. There is a possibility of privacy infringement when the data in electronic forms are given to forensic science analyst. It is rational enough to consider that forensic investigators should have right to access everything which can be helpful in tracking down the accused so that victim can get justice. But most of the time, the investigator not only takes the required information, but also all that confidential information which are not useful for the case or which has nothing to do with the case. They use it for other purpose. So, the risk of exploiting the privacy is always there in case of cyber forensics investigation.

This can be similar to controversial Aadhar Card case, When UDIAI used to collect all the information from the citizens of India on the behalf of government. So, in such cases, if any unauthorized person get access to the PIN, password, Username or such other required information because of the forensic science analyst, then it will not be difficult for them to manipulate the account and use it for illegal purposes. So, in a way we can say that if forensic investigators get access to that confidential information which is not required for the case in hand, then it should fall within the ambit of breach of right to privacy. There is a need of some regulatory authority in India which will come up with some code of conduct and give

 [ISSN 2581-5369]

certifications to the forensic investigators. This code of Conduct can also give provisions for the breach of Right of privacy of individuals whose life can get affected because of the confidential information leak.

There are already established international organizations which are regulating cyber forensics. Indian government and forensic science department can adopt the code of conduct of those organizations. It will help in speedy investigation process. One such organization which Indian forensic department should adopt is "*The International society of Forensic Computer Examiners" (ISFCE).* It is one of the most reputed organization in the field of cyber Forensics. In order to be a qualified forensic investigator one need to pass the examination and get certificate from the organization. Their certification is recognized in most of the parts of world.

The cybercrime is also systematically addressed in the *National treaty of the Council of Europe's convention on crime.* It's a multinational treaty which has addressed the issue of cybercrime along with breach of the Right to Privacy. Moreover, it has also tried to harmonize and balance the step to gather cyber forensic evidences in Cybercrime as well as giving strong code and regulations for protecting the rights of privacy of individuals. The signatory nations provide for the common ground of laws, principles and procedures along with aiding international cooperation in the investigation of International cyber-crimes. The treaty's main aim is protection of Information technology and to provide for criminal penalties in the following scenario –

- Accessing a computer without authorization or using in excess of authorization.
- Blocking data without authorization
- Interfering with the data without permission
- Interfering with a system without any authority or permission
- Misusing devices.

In addition to the above treaty there are other bilateral treaties also which protect the right of individuals in case of Cyber forensics. Also the framework of the United States- India Cyber Relationships gives detailed cooperative, investigative and security principles which is consistent with various national and international responsibilities too.

V. 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.

VI. Conclusion

In the upcoming years computers are playing a major role. In our day to day life without computer we are not going to do any work. So the increase use of technology will also lead to increase in crime rate. The cyber-crime case has to be handled very carefully in order to cull out the truth. Giving training for the police and judicial officers is very important. India has to develop a lot in handling cyber-crimes cases.

VII. 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.

 [ISSN 2581-5369]

The following are suggestions recommended:

- Internet security to be tightened
- Encryption technology to be used
- Intrusion detection systems to be used
- Cyber forensic lab should be get established in all the police stations
- Establishment of cyber courts for handling cyber-crime cases.
- Educating the public on cyber-crimes cases
- Motivating cyber-crime victims for registering complaint against the criminals.

*****

 [ISSN 2581-5369]

VIII. BIBLIOGRAPHY

(A) Articles Referred

- 'Crime in India 2014 Compendium', National Crime Records Bureau, Ministry of Home Affairs
- Ahmad, Farooq, Cyber Law in India (Law on Internet), Pioneer Books.
- Ashok KM, 'What NCRB statistics says about Criminal Justice system in India?' NOVEMBER 13, 2015, http://www.livelaw.in/what-ncrb-statistics-says-about-criminal-justice-system-in-india.
- Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Cyber Forensics"
- Governing Cyber Security in Canada, Australia and the United States on JSTOR." n.d. www.jstor.org/stable/ resrep17311.10

(B) Websites

- https://digitalguardian.com/blog/what-cyber-security.
- "U.S. Mission India FACT SHEET: Framework for the U.S.- India Cyber Relationship." https://in.usembassy.gov/ fact-sheet-framework-u-s-India-cyber-relationship.

*****