MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

A Detailed Study to Examine Digital Forensics and Cyber Security: Trends and Pattern in India

Kumar M*

Mohit Kumar, Symbiosis International University, India, Tel: 8709240015; Email: mohitaunta@gmail.com

***Corresponding author:** Zlatko Jakjovski, Institute of Forensic Medicine, Criminalistics and Medical Deontology, Medical Faculty, Univ. St. Cyril and Methody, Skopje, North Macedonia, Balkans, Tel: +38975416000; Email: zlatedr@yahoo.com

Research Article
Volume 5 Issue 2
Received Date: April 17, 2020
Published Date: May 01, 2020
DOI: 10.23880/ijfsc-16000184

Chapter- I

Abstract

Wipro has hired a forensic firm to investigate the cyber-attack on its system, which was recently reported by the industry website. Cyber forensics laboratories and cyber forensics training facilities are being set up in 13 states and union territories to check crime rates again women. In another case a gang of Chinese fraudsters did fraud of 18.6 million USD from the Indian arm of Italian company Tecnimont spa, which is considered to be one of the biggest cyber heists in the country. These are the just few instances which are mentioned to showcase the need of improved digital forensics and cyber security in India. These days' criminals usually commit crime without involving any computing device. This makes the digital forensics examiner to think which types of criminals have so much skill and ability to handle such digital evidences. In India law enforcement agencies are taking different methods for addressing the increasing load of digital evidence.

India is a democratic nation but still it finds very difficult to balance between the legal and judicial system. The law enforcement agencies are still reluctant to follow the new suits for preventing cyber-crime. In this paper an attempt has been made to showcase the present scenario of digital forensics and cyber security in India, difficulties which are being faced by legal and police department. This paper also gives a brief about the trends and pattern of digital forensics and cyber security in India.

Keywords: Digital forensics; Cyber-crime; Cyber security; Evidence

Introduction

Digital forensics refers to the process of finding and interpreting electronic data. The main goal of digital forensics is to preserve any evidence in its most original form. It is used to recreate the past events by identifying, collecting and validating the digital information. The information in digital forensics can be in discs, floppy discs, pen drive or in any digital form.

While on the other hand Cyber security refers to "the body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage and unauthorized access. Cyber security may also be referred to as information technology security."

The advancement in technology is leading to the changed nature of crime. Now the crime is no longer limited to the physical state but it is also creating problem in virtual world.

The progress in e- technology has made the government and individual's identity vulnerable to the cyber criminals. Hence, the cyber security and digital forensics comes into the picture. Digital forensics helps in joining the dots and using the data and evidence left by the cyber criminals. Cyber security on the other hand protects the networks, devices, programs and data from attack, damage or unauthorised access. The advancement of digital forensics and cyber security can ensure the safety of the virtual world from cyber crime and cyber terrorism because cyber space contains a lot of vulnerable data which can be used for anti-social activities.

Research Question

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

Research Objective

- To study about the digital forensics.
- To know the rules and laws made for digital 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.
- To understand the role of Ethical hackers and using their knowledge and expertise in making India's cyber security stronger and digital forensics much developed.

Significance of the Study

This research work will be helpful for the legislature for making suitable changes in the digital forensics and cyber security regulatory framework in India. It will help them to understand the current scenario of the trend and patterns in digital forensics.

The work will also be beneficial for the academicians, lawyers and students in understanding the trends, patterns, loopholes and rules and regulations governing the digital forensics and cyber security in India.

Finally, the research work will also be helpful to the public in understanding this new concept of digital forensics and understanding the concept of cyber security.

Research Methodology

Doctrinal and analytical method of research has been followed in this paper for conducting research by analyzing the materials which were available in the library and online journals. APA mode of citation has been used in this paper. This research project will be completed over a time period of 4 months (January – April 2020).

Sources of Data

Primary as well as secondary sources of data have been used in this paper. Primary data includes various constitutions, legislations, judicial decisions of different nations and International conventions. The researchers has also used secondary sources of data such as books, various national and international journals , articles and materials available on the internet.

Review of Literature

Computer Forensics Characteristics and Preservation of Digital Evidence

The author of this article has talked about proper handling of digital evidence and the role of digital forensics laboratories. But the author has not compared it with the governmental rules and regulations and it does not talk about the need of digital forensics in the judicial system. The researcher is going to bridge this gap.

A Study to Examine the Cyber Forensics

Trends and pattern in India, This research article focuses on the trends and patterns on the cyber forensics in India. It talks about the role of parliament and police system but it doesn't give any suggestions about how to tackle those problems. It also doesn't talk about the role of ethical hackers in improving the quality of digital forensics in India and making the cyber security very strong.

Unpacking the International Law on Cyber Security Due Diligence

Lessons from the public and private sector - This article reviews the arguments surrounding the creation of cyber security due diligence norm and talks

About the public and private sector responsibilities in cyber space. The researcher is going to take the help of this article to explain that why Indian cyber security and forensics

are lagging behind from the western countries.

Building Foundations for Digital Records Forensics

A comparative study of the Concept of Reproduction in Digital Records and Digital Forensics - This article facilitate the proposal of a new discipline called digital records forensics, with special emphasis on digital management. The researcher tries to find out the development of this new discipline of digital records forensics.

The Basics of Digital Forensics

The primer for getting started in digital forensics – This book is written by John Sammons. It provides the foundations for people new in the field of digital forensics. This book teaches how to conduct examination by discussing what digital forensics is the methodologies used the key tactics and the tools needed to perform examination.

Guide to Computer Forensics and Investigation

This book is written by Amelia Philips, Bill Nelson and Christopher Steuart. It talks about hi-tech research and investigation from acquiring digital evidences to reporting its findings.

The researcher of this paper has used this book to compare the technologies used by the Indian investigation department in conducting digital forensics examinations.

Chapterization

The entire research work will run into five chapters.

Chapter I- Introduction

- Chapter I will be on introduction and it will bring out the importance of study, and states its objective, methodology, significance of the study, sources of data and the literature review.

Chapter II-Concept of Digital Forensics and Cyber Crime

- Chapter II will contain the meaning and understanding the concept of Digital forensics and Cyber-crime.

Chapter III- Right to Privacy in Digital Forensics and Cyber Security

- Chapter III will apply the principle of right to privacy in Digital Forensics and try to critically analysis the concept with the help of international treaty and conventions.

Chapter IV-Comparative Review of Legal Regimes of Cyber Forensics Among Nations

- Chapter IV will try to compare the established legal regimes in the area of cyber forensics in various nations of the world.

Chapter V – Conclusion and Suggestions

- Chapter V will give conclusion and suggestions followed by Bibliography and references.

Chapter – II

Concept of Digital Forensics and Cyber Crime

What is Digital Forensics?

It is the process of preserving, identifying, extracting and documenting the computer evidence which can be used in the court of law. It can also be termed as "Science of finding evidence from digital media". It helps forensic team by providing best techniques and tools to solve complex digital-cases.

Brief Landmark on the History of Digital forensics –

The foundation of digital forensics started in 1840s when Hans Gross (1847-1915) became the first person to use scientific studies in the criminal investigation. Later in 1942 FBI in the USA set up a forensic laboratory to offer forensic services to all local authorities.1978 was the year when first computer crime happened and Florida Computer Crime Act came to force. The term Computer Forensics was used in the literature for the first time in the year 1992. This helped in the formation of International organisation on Computer Evidence (IOCE) in the year 1995. The digital forensics came to prominence in the year 2000 with the establishment of the first Regional computer forensic laboratory by the FBI. All this resulted into the publication of first book by the Scientific Working group on digital evidence (SWGDE), called "Best Practices for Computer Forensics" in the year 2002. In the year 2010, Simson Garfinkel incorporated digital evidences in the forensic investigation processes.

Steps of Digital Forensics

- **Identification-** This is the first step in the process of digital forensics. It involves the identification of the

purpose of investigation and various resources required for the completion of the investigation.

- **Preservation**- In this step data is isolated and preserved so that it can be used for further investigation.
- **Analysis** - It identifies the tools that can be used, process the data which is preserved in the second stage of digital forensics and then analyse the data.
- **Documentation**- It involves documentation of the crime scene such as taking photograph, sketching and crime scene mapping.
- digital forensics investigation.

Types of Digital Forensics

- **Disk Forensics** - It extracts data from storage devices by searching active, modified and deleted files from the storage device.
- **Network Forensics** – It studies computer network traffic and collect digital and legal evidences.
- **Wireless Forensics** – It analyzes and collects the data from wireless network traffic.
- **Database Forensics** – It studies and examines databases and their met data.
- **Malware Forensics** – It studies the identification of malicious code, viruses and other payloads.
- **Email Forensics** – It studies the recovery of deleted and modified emails.
- **Mobile phone Forensics** - It is the examination and retrieving of call logs, deleted call and other potential forensic evidences from the device.

The common examples of digital forensics can be theft of intellectual property, Bankruptcy investigation, Forgery cases, industrial espionage, fraud investigation, blackmailing cases, pornography cases and other various crimes which involves digital media platform.

What is Cyber-Crime?

It is an unlawful action against any person or community using computer, its system and its online and offline applications. In this type of crime, Information technology is used to commit and cover any offences. But in this type of crime mens area is compulsory and if the action is unintentional then it will not fall within the ambit of cyber-crime.

Some common examples of cyber-crime can be distribution of child pornography, accessing dark web, software piracy, industrial spying etc.

Some Common Types of Cyber Crime are as Follows-

- **Hacking** – It's an unauthorized access to a computer system and network.
- **Spoofing** – It is changing the identity of one computer or network and pretending it is some other computer or network.
- **Phishing –** It's an act of getting confidential information from bank or other financial institutions by using illegal ways.

Common Cyber Crime Tools Which is Used in Digital Forensics-

KaliLinux – It is software which is maintained and funded by offensive security. It's specially designed software used in digital forensics and penetration testing.

Ophcrack - It's used for cracking the hashes, which are generated by the same file window and helps in securing GUI system which allows any system to run on multiple platforms. EnCase – It is a shared technology among various digital investigation products. It comes in various ranges which is designed for forensics, cyber security and security analytics.

Scope of Digital Forensics in Cyber-Crimes –

Until recent time, digital forensics used to cover crime related to computer applications and software. But now with the increasing popularity, social media is also becoming a place where crimes are happening at a fast pace. The forensic laboratories along with developed technology are helping in tracking criminals in very less time. For example, with the help of EnCase, forensic investigators can track the IP address and reach to the culprit. Furthermore, Ethical hackers can also help in infringing into the computer system of suspected criminals and gather evidences.

Chapter- III

Right to Privacy in Digital Forensics and Cyber Security

Whether the Acquiring of Digital Forensics by the Investigation Officer Amounts to the Breach of Right to Privacy?

When it comes to the development of Digital forensics in India, there is not even a single codified law which deals with

this aspect of forensic department. This can be due to the fact that technology law is still in its nascent stage in India. There is no regulations governing digital forensics, so if someone wants to become a cyber forensic, he simply has to complete certified course on digital forensics after finishing his graduation. There is no organisation who governs the profession of digital forensics in India. The primary use of digital 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 be relied about 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 guaranteed under the constitution of India. There is a possibility of privacy infringement when the data in electronic forms are given to forensic science analyst. It is reasonable enough to consider that forensic investigators should have right to access everything which can be helpful in tracking down the culprit. But most of the time, the investigator not only takes the required information, but also all those confidential information which are not needed for the case. They use it for other purpose. So, the risk of exploiting the privacy is always there in case of digital 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 to 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 organisation in India which can come up with some code of conduct and give 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. There are already established international organisations which are regulating digital forensics. Indian government and forensic science department can adopt the code of conduct of those organisations. It will help in speedy investigation process. One such organisation which Indian forensic department can adopt is "The International society of Forensic Computer Examiners" (ISFCE). It is the most reputed organisation in the field of computer Forensics. In order to be a qualified forensic investigator one need to pass the examination and get certificate from the organisation. Their certification is recognised in most of the parts of world.

In the landmark case of United States V. Ivanov, the court addressed the subject matter of those computer crimes which was performed by those internet users which were outside the United States and did not fall within the ambit of American court's jurisdiction. Some users did unauthorised access on US servers from Russia. The investigation officer of US used the court's order to authorize remote access to Russian server, which led to the imprisonment of Ivanov, without Ivanov consent. In response to the actions of investigating officers of US, the Russian State security filed a criminal case for unauthorized illegal access without proper authority.

The cybercrime is systematically addressed in the 52- Nation treaty of the Council of Europe's convention on crime. It's a multinational treaty which addressed the issue of cybercrime along with breach of the Right to Privacy. It tried to harmonize and balance the step to gather digital 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 sui generis protection relating to Information technology provide for criminal penalties in five categories –

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

In addition to the above treaty there are other bilateral treaties 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.

Chapter - IV

Comparative Review of Legal Regimes of Cyber Forensics Among Nations

Whether there are any Established Legal

Regimes for Digital and Cyber Forensics among Nations?

Municipal laws reflect different notions on the rights of states, need of public security and balancing it against the security of private individuals. The comparison of Municipal laws can help in adopting better digital cyber forensic practices and avoiding failed attempts practiced by other nations. It can help in the identifications of major challenges which are common in the various states digital forensics practices.

Hong Kong Special Administrative Region, China

It reflects the transformation of British common law to the laws of People's Republic of China. The academic circle and the law enforcement agencies have focused on cyber security and digital forensics. The big data analytics has been used by the private users and the government organisations in China. They have personal data privacy ordinance which is similar to the European Union. It helps the private data users to protect their digital content and digital data. The big data analytics of Hong Kong is going will impact the General Data Protection Regulations (GDDPR) for EU citizens regardless of their locations. The Personal Data Privacy ordinance aims to balance the data protections rules of Hong Kong and EU. The law enforcement agencies of Hong Kong have established computer forensic labs and it also publishes report on cyber forensics crimes.

The Republic of Korea

South Korea collects its data about criminal justice from its own criminal justice portal. Korean University also launched its first domestic digital forensic research centre. It released its first digital evidence guidelines on cyber-crime in 2006. It aims to identify common standard procedure to fight cyber crimes and better forensic investigation. Korea has very strong hacking and data protection laws when compared to other nations of the world.

The United States of America

US constitutional laws do not allow unreasonable state searches after its fourth amendment to the constitution. The Supreme Court has held that without strong and sufficient cause the search and seizures of digital evidence are in violation of law and also violate the reasonable expectations of privacy. The federal cases after analysing digital forensic issues found that the most common attacks are on the legality of digital forensic use. Such unreasonable searches can lead to civil as well as criminal damages. So, the judiciary of USA take necessary step to protect the privacy of its citizens and provide guidelines for digital forensic investigation.

As you can see the above three countries have proper legislations for governing cyber and digital forensic laws. Hong Kong have personal data privacy ordinance, Korea has its own domestic forensic laboratory, and The United States also have digital forensic laboratories which are managed by FBI. Further, the judiciary of these countries are really active when it comes to tackling new problems which the citizens are facing because of crazy growth of digital world. They are relating the concept of privacy and reasonable search and seizure with the digital forensic investigations. But on the other hand, India is lagging behind the active application of jurisprudence with the digital forensics. Technology is still at its nascent stage but India is also becoming hub of cyber-crimes. Social media is becoming a tool of spreading rumours and creating riots among communities, innocents are getting blackmailed, forgery cases are happening etc. All this makes it necessary for the legislation to come up with strong code of conduct which will govern the working and process of digital forensics in India. The development of digital forensics in India can help in speedy trial and delivery of justice. There are lot of hackers out there who are using confidential data to commit fraud and manipulate innocent citizens. India also do not have any strong punishment for cyber-crimes which can act as a deterrent.

Chapter –V

Conclusion and Suggestion for Developed Digital Forensic Department in India

From the researcher's point of view, In a country like India where government is focusing on Digital India projects, there is an urgent necessity of a legislation or a regulatory body which can ensure quality, conduct and ethics in the digital forensics department of India .As, mentioned in chapter III, India can adopt code of ethics and regulations from various treaties like 52- nation treaty or establish organisation like International society of forensic computer examiners. According to Centre for Advanced Research in Digital Forensics and cyber security, India is third most vulnerable country for cyber threats. The Indian forensic department should establish more technology updated labs which can be used for dedicated research and provide development facility for Digital Forensics professionals. Law enforcement agencies should work together with these forensic organisations to keep digital and cyber-crime at bay. The forensic professionals should be taught ethical hacking. It will help them to get acquainted with the little complexities of Cyber-crime. It can also help them in finding loopholes and can come up with strong code to protect the data of private individuals and organisations in the cyber world. There should be a continuous criminological and logical research for the identification of vulnerabilities and threats in the

digital world. The forensic laboratories can educate the young mind in various educational institutions and try to mitigate them. The law enforcement agencies should assist the digital forensic laboratories to assist them in developing them according to global standards. They should deal with varied sets of data, research, survey, trends, pattern and various cyber threats; it can help them in informed decision about cyber security and digital forensic needs. There should also be an introduction of forensic science curriculum in law and engineering colleges in India. There should also be a clear separation of crime investigation from law and order duties, so that the forensic investigation will not be delayed because of not so necessary formal duties

Bibliography

Books

- Amelia Philips , Bill Nelson and Christopher Steuart, Guide to computer forensics and investigation (2009)
- B.R. Sharma, Forensic Science in Criminal Investigation & Trials (2018)
- John Sammons, The basics of digital forensics: The Primer for getting started in digital forensics (2011)

Research Papers

- "Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics on JSTOR." n.d.
- www.jstor.org/stable/23079051.
- "Computer Forensics: A Pocket Guide on JSTOR." n.d. www.jstor.org/stable/j.ctt5hh5mg
- "Computer forensics : Characteristics and preservation of digital evidence . FBI Law Enforcement Bulletin." n.d.
- https://www.fbi.gov/publications/leb/leb.htm
- "Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. In Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence on JSTOR." n.d.
- www.jstor.org/stable/10.7249/j.ctt15sk8v3.1
- "Fostering the advancement of Internet of Things on JSTOR." n.d.
- www.jstor.org/stable/23079051.
- "Governing Cyber Security in Canada, Australia and the United States on JSTOR." n.d. www.jstor.org/stable/resrep17311.10
- "Riding the digital wave: The impact of cyber capacity building on human development on JSTOR" n.d.
- www.jstor.org/stable/resrep07069.7
- "The interface between forensic science and technology: How technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system. Philosophical Transactions: Biological Sciences on JSTOR" n.d. www.jstor.org/stable/24505157
- "Unpacking the international law on cyber security due diligence: Lessons from the public and private sectors on Chicago journal of International Law." n.d.
- https://chicagounbound.uchicago.edu/cjil/vol17/iss1/1/

Websites

- Full list. (n.d.). https://www.coe.int/en/web/conventions/full-list/- /conventions/treaty/185
- "Korea releases guidelines on cyber crime, by Yoo Y" https://www.zdnet.com/article/korea-releases-guidelines-on-cyber-crime/.
- "Personal Data Privacy Ordinance of Hong Kong." http://www.edb.gov.hk/attachment/en/sch-admin/admin/about-sch/personal-data-ordinace-cap486-note/privacy.
- "Report, Inter-departmental Working Group on Computer Related Crime, Hong Kong". https://www.infosec.gov.hk/english/ordinances/files/computerrelatedcrime&uscore; eng.pdf.
- "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/
- "What is Cyber Security? Definition, Best Practices & More."
- https://digitalguardian.com/blog/what-cyber-security.
- "What is digital forensics?"
- https://www.computersciencedegreehub.com/faq/what-is-digital-forensics/.

References

1. (2019) What is Cyber Security? Definition, Best Practices & More.
2. Mendonca J (2019) Wipro hires forensic firm to probe cyber-attack.
3. The Economic Times (2020) What is Insider Trading? Definition of Insider Trading. Insider Trading Meaning - The Economic Times.
4. The Economic Times (2020) The biggest digital scam - The Economic Times.
5. Mercer LD (2004) Computer forensics: Characteristics and preservation of digital evidence. FBI Law Enforcement Bullentin 73(3): 28.
6. Iitmjanakpuri.com. (2020).

7. Shackelford SJ, Russell S, Kuehn A (2016) Unpacking the international law on cyber security due diligence : Lessons from the public and private sectors. Chicago journal of International Law 17(1): 1-50.

8. Xie Sherry L (2011) Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics. The American Archivist 74(2): 576-599.

9. Pam (2018) What is Digital Forensics?

10. Pam Supra note 9.

11. (2020) What is cybercrime ? Types, Tools , examples. Guru 99.

12. United States V. Ivanov , 175 F. Supp. 2d 367 (D. Conn . 2001).

13. Full list. (n.d.).

14. US Mission India (2016) FACT SHEET: Framework for the U.S.-India Cyber Relationship.

15. Personal Data Privacy Ordinance of Hong Kong. Accessed from

16. Hong Kong. Report, Inter-departmental Working Group on Computer Related Crime.

17. Yoo Y (2006) Korea releases guidelines on cyber crime.

18. (2017) The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team. Fostering the advancement of Internet of Things.