IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

DEVELOPMENTS IN CYBER FORENSICS IN INDIA: COMBINING LEGAL FRAMEWORKS WITH TECHNOLOGICAL INNOVATIONS

[1]Ms. Muskan,[2]Prof.(Dr) Somdut Bhardwaj,

[1]Research Scholar,[2]Dean

[1]Amity School of Law, [2]Amity School of Law

[1]Amity University, Manesar, Haryana, [2]Amity University, Manesar, Haryana

Abstract : The swift proliferation of digital technologies has necessitated the evolution of robust cyber forensic frameworks within legal structures worldwide. It was in late 2000s that the Indian subcontinent realised the value of the forensics in the digital medium with the incident of the Taj Hotel. Supplementing legislative reforms, India has established the specialized structures within its premier forensic evidence examination agency under National Forensic Science Labs, to address cybercrimes. Remarkably, the Cyber Crimes Research and Development Unit (CCRDU) and the Cyber Crime Investigation Cell (CCIC) have been instrumental in collecting information on cybercrime cases and conducting investigations, respectively. These units play a pivotal role in coordinating with state police forces and other organizations to combat cyber threats.

The paper follows the approach of analysing the secondary data wherein, the cybercrime statistical data, released by the NCRB (National Crime Records Bureau) has been utilised to bring out the current picture of such crimes in India. In support of the same, the procedure that been followed in the forensics labs with respect to the digital evidence has also been examined.

The paper highlights the aspect of the forensic labs being not equipped with the required softwares for the examination, leading to the misleading results from the evidences. Apart from this, challenges persist including the need for continuous upskilling of law enforcement personnel and ensuring the examination of evidence in the correct manner.

This paper in the whole provides a comprehensive analysis of India's current cyber forensic framework, evaluates the effectiveness of recent initiatives, and proposes recommendations to fortify the integration of cyber forensics within the Indian legal system.

IndexTerms **– Cyber Crime, Cyber Forensics, Investigation & Technology.**

Introduction

The use of technology in every sector along with the internet services has made the pace of work faster. Along with the pace in the online activity, the pace of cyber crime has also increased and to tackle the issue of such crimes, the development of cyber forensics was done. For the purpose of identifying the cyber criminals, this field was developed and now has become an integral part of the judicial system. The types of crimes that fall under this category have a basic need to be examined with due care and tools and techniques, which help in excavating proper results. It is at this place, where the crimes that are executed on the computer along with the internet attached to it, fall under the ambit of the computer forensics. The term cyber forensics is the synonym for the words digital forensics and computer forensics and can be used alternatively. Looking at the aspects of the computer forensics, the procedure starts at the point where the evidence is lifted from the crime scene, where the member of the cyber forensic team arrives and uplifts the evidence with the help of tools and software and share the same with the forensic lab expert, who in turn examines the evidence and creates a chain of custody. The procedure of examination depends on the nature of the evidence. Thus, it is important to note that if the evidence is not collected, examined or analysed in the correct manner, then it may cause deviations in the reports of the evidence that is presented in the courts, resulting in clear denial of justice to the aggrieved.

The relevancy of the digital evidence has increased over time, as the use of electronic devices with internet attached to it has become an integral part of today's life. However, at this stage it is even the user who is unaware about the fact that his personal information is already been collected and stored in his device without his consent. For example, when we go for window shopping online, the entire data (search history) is stored

on our devices, and when we search for any news article or even run of social media accounts the adverts of the same products that we just viewed come up in the pop up form in the same. This is because our information is stored and utilised by the search engines. It is this information that is stored in the device, when is accessed by the experts play a major role in framing the report of the electronic evidence. There are various steps involved in the investigation mechanism of the electronic evidence: right from extracting the evidence from the source to storing it for future reference. The entire process of scrutiny involves a variety of tools and techniques depending on the type of evidence. Not only this, their relevance stays for a longer period as they can be referred in any case depending on the situation. There are challenges in this sector related to technology that is required to examine the data, acute shortage of the experts and their expertise apart from the fact that there is no fixed roadmap for such process.

The need for the cyber forensics was felt when the Taj attacks took place in India in 2008. The perpetrators found the Indian market weak in terms of cyber development, which helped them succeed in the commission of crime. For example, in order to commit crime, the perpetrators needed information, hence before searching for their required information, they targeted the electronic systems such as computers which would track their search patterns and paved ways for themselves by taking an under path for the same. They not only took an under path for their activities, but also managed to hack these systems which would, in their true course track them in their search patterns. Thus, they managed to flee the air traffic control and other telecommunication networks paving way for their works. It did not end only here, their financial transactions, the money from *hawala* also could not be traced down, as they had cracked the path to cover such transactions too, which came from other countries. Hence, all information was collected, stored and analysed by them without coming under the scrutiny.

In the Ajmal Amir Kasab Vs State of Maharashtra[1], 2008, it was noticed that the terrorists had stolen the data of the computers installed at the hotel so that they can get the information of the dignitaries that were present in the hotel at the time of attacks. This proved the aspect of their preparedness when it came to stealing the data and committing the terrorist attack. The key victims belonged to the country US and London and were their targets. Not only this, at the time of scrutiny of the electronic evidence, it was found that the movements of the dignitaries were also tracked in the hotel in order to run them down. The terrorists were updated with the advanced technology and relied upon the internet phones and connected with their handlers at the base in Pakistan. Not only this, the perpetrators used global positioning system to evade their tracking from the Indian authorities. They also used the google earth to track every path to the epicentre of the attack. Apart from this, the handlers were informed of the movements of the security forces, by the help of the media that was present at the precincts of the hotel and was informing about the steps that the forces were carrying out. Hence, it concluded the fact that the knowledge on the part of Indian authorities with respect to the tracking of the culprits was not upto the level of the culprits.

Post the 26/11 attacks, the central government of India took several steps to enhance the intelligence security of India such as enhancement of surface and air surveillance by Indian Navy and coast guard ships and aircraft along the coast and in all offshore development areas. Another step that the government of India took to upgrade the security was by establishing National Command Control Communications and Intelligence (NC3I) Network as a part of the maritime security measures[2].

Limitations

The paper examines the issue of cyber crime with respect to the Indian subcontinent only. The crimes that are committed on the electronic device, namely computer is only examined in the course of research here. Also, the paper focuses on the statistical data of years 2020, 2021 and 2022 only in terms of timeframe. The analysis of the crime records has been obtained from NCRB, as it is a reliable source of data in terms of crime records. The secondary data with respect to the cyber forensics has been obtained from published articles and reports from various ministries such as MHS, MeITY etc.

[1]Kahn J. Mumbai Terrorists Relied on New Technology for Attacks. The New York Times [Internet]. 2008 Dec 9; Available from: https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html

[2]Home. Q 6. After 26/11, what steps have been taken to strengthen the intelligence system and surveillance? | Ministry of Defence [Internet]. Mod.gov.in. 2023. Available from: https://mod.gov.in/faqs/q-6-after-2611-what-steps-have-been-taken-strengthen-intelligence-system-and-surveillance

Legislative and Institutional Frameworks

i. Overview of cyber laws in India (IT Act, 2000, and amendments)

It was in 1990's where the internet made its place in the Indian markets. The main objective of introducing the act was to provide legal recognition to all the transactions that were carried out in the form of electronic communication and electronic data exchange. This was further expanded in the form of electronic commerce, and made its way in terms of creating, storing and analyzing the information that was generated on the electronic devices with the help of internet. Over the passage of time, the act introduced many amendments to keep up with the demands of the society. On November 31, 2024 the union ministry of electronics and technology enforced certain amendments with respect to the penalties and certain acts, a few of them are:

- Under section 66A, which talked about the "offensive" messages has officially been struck down from the act after the Supreme Court ruled the same as unconstitutional in the Shreya Singhal case in 2015.

- The penalty under section 69B, which talks about sharing the information from the intermediary's end to the authorised government agency about their services and not complying on the orders of the same to them now calls for a penalty of ₹ 1 crore, previously which was not defined in the section and only carried out a imprisonment of 3 years.

- Under section 72, if any person discloses the information that it has obtained under the powers conferred to it, and shares the same to a third party, without the consent of the concerned person, shall attract a penalty of up to ₹25 lakh.

- Under section 44, failure to comply by the orders of the controller of the certifying authority shall attract a fine up to ₹15 lakh and delay for the same shall attract a fine of ₹1.5 lakh on per day basis.

- In section 70B, which talks about the Indian Computer Emergency Response Team (CERT-In), non-compliance to the orders of the authority shall attract a fine of up to ₹1 crore and shall also carry imprisonment of 1 year[3].

In the same flow, where we talk about the cyber crimes and their penalties being increased to enhance their imposition on the parties, the government of India has also been looking forward towards the expansion of national forensic science labs in India. The labs have been designed in order to examine the electronic evidence which yield specialised testamentary verification in court of law. In terms of examining a electronic evidence, a chain of custody is prepared and this is presented in the court of law. In the same, the government of India has established Cyber Crime Research and Development Unit (CCRDU) and Cyber Crime Investigation Cell (CCIC). The CCRDU works as a bridge between the state police forces. It basically maintains the track record of the cyber crime data and the cases that have been reported to the police for investigation. The CCIC was established in 1999 and holds jurisdiction all over India. The organization works under the Information Technology Act, 2000 and also works in collaboration with the Interpol to provide the information of the cyber crimes to India[4].

Cybercrime Trends in India

i. Analysis of secondary data from NCRB reports[5]

- In 2020, there were maximum cases from Uttar Pradesh and Karnataka in the category of states. In 2021, the record was maintained by Telangana state with 10,303 cases followed by state of Uttar Pradesh with 8829 cases. In 2022, the number of crimes increased by 12556 numbers, a major contribution by Karnataka and Telangana remained again at the top with 15297 crimes reported.

- There was an overall jump of 2722 cases in 2021, and the same was found to be more than double in 2022, with numbers 12,477, with a significant rise of 24.4%, with respect to the data representing all Indian states.

- In 2019, there was a sudden rise in crime from Telangana, previously record was held by Uttar Pradesh.

[3]Agrawal A. Amendments to IT Act decriminalise offences, increase penalties [Internet]. Hindustan Times. 2023 [cited 2025 Mar 16]. Available from: https://www.hindustantimes.com/india-news/amendments-to-it-act-decriminalise-offences-increase-penalties-101701517892813.html

[4]Shekhawat H. "Digital Evidence and Cyber Forensic Procedure and its Role in Criminal Justice System" [Internet]. Available from: http://www.penacclaims.com/wp-content/uploads/2020/04/Hemangini-Shekhawat.pdf

[5]INCREASE IN CYBER CRIMES [Internet]. pib.gov.in. Available from: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505

Digital Evidence and Examination Procedures

i. Standard procedures followed in forensic labs

These crimes emerge from gadgets, with the help of the internet and have no fixed territorial boundaries. Another issue that needs to be addressed is the investigation process. The software, tools, and expertise need to be broadened as the crimes are more heinous than they seem. There are instances, where the experts are unable to file a report due to the lack of technology that was needed to inspect the evidence. This means that there is a deficiency in terms of the investigation procedure. Electronically generated evidence has worth only when it is examined carefully by an expert and is presented by them in the court. The facts that arise out of the evidence tend to change the course of a case and also define the modus operandi at times. The experts that preside over in the cyber branch of law and order, examine the data provided and perform the duty of an expert in the court. The evidence is collected, examined, and analyzed, and then a report is prepared which is then exhibited to the judge. The procedure not only ends here, but the documentation process is also further carried out in the name of storage. The evidence, in the original form, is stored for further reference and is disposed off after the passage of a certain time. All this can be categorized into certain steps which are defined below.

i. **Identification** of the digital evidence for its scrutiny is one of the most important steps. It is this step which when carried out, will aid in classifying the evidence, its nature, the process of scrutiny, the documentation work, and its final presentation in the court. In this phase, the information is obtained about the cybercrime and it also helps in facilitating the case by pointing out the evidence, and categorizing it under the value, as to which one is more important, and placing them according to their relevancy[6].

ii. **Preparation** is the next step after brainstorming and finding out the relevance of the evidences. It simply means to have all the equipments tools care and steps to be followed to mine out the evidence from the place of the crime. The purpose of this phase is to make sure that the operation and infrastructure can support the investigation. The preparation phase can be divided into preparation, case evaluation, and preparation of detailed design for the case, preparation of investigation, and determination of required resources[7].

iii. **Evidence preservation** means to keep the evidence in the same, in which it was found. This is necessary to perform, because if by chance, while uplifting the evidence, whether a gadget or the evidence of soft form, gets damaged, then the proceedings may get affected. First responders, investigators, crime scene technicians, and/or digital forensics experts must demonstrate, wherever possible, that digital evidence was not modified during the identification, collection, and acquisition phase, the ability to do so, of course, depends on the digital evidence & circumstances encountered by them. For this, a chain of custody has to be maintained, which is helpful for further use. The chain of custody is the process by which investigators preserve the crime (or incident) scene and evidence throughout the cycle of a case. It includes information about who collected the evidence, where and how the evidence was collected, which individuals took possession of it.

iv. **Collection of the data** or the gadgets is done by the investigators who are actually the first responders at the crime scene. It may involve removing the evidence from the crime scene and then imaging, copying, or printing out its content[8]. Cybercrime cases have no fixed location for the commission of the illegal activity and this is the key reason why the targets can be present in any part of the world. The cybercrime scene also includes the digital devices that potentially hold digital evidence, and spans multiple digital devices, systems, and servers. The crime scene is secured when cybercrime is observed, reported, and/or suspected.

v. An **analysis** is an in-depth search of evidence relating to the incident being investigated. The outputs of examination are objects and collected information; they may include system-and user-generated files. The analysis aims to draw conclusions based on the evidence found[9]. Investigators analyze digital copies of storage media in a sterile environment to gather the information for a case.

vi. **Documentation**: Examiners should keep in mind that all the relevant details are shared correctly and there should be no point left out related to the process carried out. One of the issues that might be questioned is the duration clause with reference to the analysis. The time carried out must be present in the written form along with the tools and their usual tie and the time taken in the case. This means that the case must present itself with all the minute details which if left out may divert the judgment.

vii. **Preservation** is the last step of the case. Here the file that has been created is presented in the court. The contents of the file can roughly be: Chain of custody, seeking court permission for examination of the

[6] Kiener-Manu K. Cybercrime Module 6 Key Issues: Handling of Digital Evidence [Internet]. www.unodc.org. 2019. Available from: https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[7] Digital forensics [Internet]. OpenLearn. 2011. Available from: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1

[8] https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1 as accessed on 22 Jun 2021

[9] Digital forensics [Internet]. OpenLearn. 2011. Available from: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1

document, evidence details, evidence attached to the file or in the envelope form, place of reporting, written submissions, approved documents such as seeking permission for officials to examine, team permission, tool, and technique permission, transfer permission, original evidence record in written form, and any other document that was created in due process.

Challenges in India's Cyber Forensic Framework

i. Insufficient training and skill development for law enforcement: The answer to every question lies in the knowledge of the situation. If we possess the knowledge of any provided issue it can be addressed. The same applies in the context of crimes pertaining to cybercrime. This transaction is two ways. The authorities and the government should work hand-in-hand to provide knowledge and the masses should ponder towards such measures undertaken so that they can be cautious about the ongoing trends in the criminal market and can save themselves from being trapped. The consumer/customer should take part in the discussion/educational program such as seminars, workshops, training camps for the public, debates, etc. The ongoing program should include people from the general public, address their queries, and should formulate an environment where the users feel comfortable to share their issues. Results of the discussion serves in two ways: it provides feedback on the previous sessions and the questions that arise from the public, guides them to introduce new measures that must be adopted to tackle the cybercriminal cases. When the public can relate their issues or any such incident that they faced in the past and the same was discussed in the seminar, it helps in increase of knowledge and also warns them for such similar future incidents.

ii. **Licensing policy for software:** The use & development of software by hackers is another subject that desires attention. The softwares so developed by them are quite strong and the coding involves a skilled person. If the development of such software is regulated then the chances of such crimes can be lessened. If there is a strong licensing policy on the production of such tools than somewhere or the else advance the crime, then the situation of victimization of an individual also lessens. The software that especially disables or helps indirectly in erasing the network route of the device such as computer proves to be fatal in certain cases. The software's that are used to erase data's are sometimes tough to detect by the professionals owing to their strong development. The same can be erased, when the authority to manufacture, develop or procure any such tool used in their making is brought under the control of the authorities.

iii. **Coordination issues between State and Central authorities:** The authorities that analyze or examine the evidence are dependent on the first responders. They can only check and report the evidence so brought to their notice, but at times there are shreds of evidence that are not brought to the eyes of the investigator and it may hamper the process. The experts must be allowed directly to visit the crime scene as and when needed, and also they must be free to carry out any kind of test on the data or the device. After preparation of a copy, the duplicate should be in the authority of such people and they must be free to use any software or tool that they may think fit to be applied in such cases.

Recommendations and Future Directions

i. Upgrading forensic labs with advanced tools and software

The forensics labs must be equipped with new technology and softwares that can help in collection of evidence from the crime scene as that is the most important aspect of any case related to cyber crime. For example, if there is any device that is involved in any case and is present at the crime scene, the first step that accounts for is to check whether it is currently in a working stage or has been shut down before the team arrived. If there is condition that the system was connected to the power, then proper steps must be carried out to confiscate the evidence because in terms of extracting the evidence from the crime scene, the ROM i.e., the Read Only Memory, which gets erased once the system is shut down, hence this must be kept in mind by the crime team. Apart from this, when the team is present at the scene, the team must be equipped with all the softwares that maybe required transporting the device safely from the crime scene to the Forensic Lab.

ii. Policy recommendations for legal and procedural enhancements

As of the latest press release by the PIB, three new Central Forensic Labs have been established at Bhopal, Guwahati and Pune and efforts have been made in enhancing the lab that was established at Kolkata[10]. Financial investments have been made in Narcotic Drugs & Psychotropic Substances, Digital Forensics, DNA Forensic analysis, Forensic Psychology. In order to address the necessity for capacity building of manpower in forensic sciences, MHA is undertaking training for Investigating Officers, Prosecutors, and Medical Officers from States/UTs in collection, storage and handling of DNA evidence and use of Sexual Assault Evidence Collection Kits. So far 32,524 Investigating Officers, Prosecutors and Medical Officers have been trained. The Ministry of Home Affairs has also distributed 18020 Sexual Assault Evidence Collection Kits to the States/UTs as part of this training.

[10]FORENSIC LABS [Internet]. Pib.gov.in. 2024 [cited 2025 Mar 16]. Available from: https://pib.gov.in/PressReleasePage.aspx?PRID=2085688

iii.Future roadmap

With the enactment of the new Criminal Laws which mandates forensic investigation for offences involving punishment of 7 years or more, a significant increase in the workload of forensic science laboratories is expected. To meet this heightened demand, significant investment and enhancement in the national forensic infrastructure is imperative. Establishment of additional off-campuses of the National Forensic Sciences University (NFSU) and Central Forensic Science Laboratories (CFSLs) is essential to address the shortage of trained forensic manpower, alleviate the case load / pendency of forensic laboratories.

Conclusion

Hence, the paper outlines the importance of cyber forensics with respect to the use of technology and presentation of the evidence correctly in the court. The succession of any case lies in the efforts put by the authorities. The authorities can be set free by the government to carry out necessary operations on the shreds of evidence and the feedbacks of such experts must be timely availed to the government so that it can draft acts or laws for the facilitation of such needs. The timely feedback on the pattern of crimes can also help the government to roll out necessary steps to the authorities and the people of India. The past incidents have served as learning for the authorities and the same will be for the future if the service remains constant. The forensics should also be treated as an integral part of the investigation and its needs should be addressed timely and in the best possible manner, only then a nation can be classified as secure.