NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 2, Issue: 2
July-December 2023
E-ISSN: 2584 - 0924

CRIMINAL INVESTIGATION OF ELECTRONIC EVIDENCE: CHALLENGES FACED WITH DIGITAL FORENSICS

Ms. Sadhna Gupta[i] & Ms. Meghali Das**[ii]*

Abstract: *Investigation of a crime scene involves recognizing potential evidence, their collection, preservation and then sending the same for analysis by experts. Forensic science refers to the application of scientific practices during collection and analysis of such evidence, while adhering to the standards of criminal procedure and admissible evidence. It plays a major role in the criminal justice system and requires utmost precision, knowledge, and care by the law enforcement agencies as well as forensic experts. However, with the advent of technology and its integration into the daily life of every person, a new avenue for commission of crimes has opened, which is known as cyber-crime. In simple terms, any harmful act that has been committed using specialised knowledge or use of computer technology is called cyber-crime. "Computer" herein refers to any electronic device, be it computers, cameras, smart watches, mobile phones etc. that can store data in some form. As society's dependence on computer systems increases, the need for protection against cyber-crimes and cyber criminals increases.*

1. INTRODUCTION

There are four main dissimilarities between cyber-crimes and other crimes. They are:

- Committing a cyber-crime is much easier to learn than other crimes.
- Compared to the potential damage that is caused by cyber-crimes, the resources required to commit such crimes are much less.
- Physical presence of the perpetrator is not needed in the place where the crime is being committed.
- The illegality of such a crime is often not very clear.

However, the problems emerging from cyber-crime are not limited to only the digital world, but have added new dimensions to the commission of traditional crimes as well. Thus, two broad categories of crime involving computers can be identified in contemporary times. Firstly, crimes targeting the computer itself, which are committed purely in the digital world or cyberspace. And secondly, crimes that use computers as an aid to committing another crime in the real or physical world. In both instances, sophisticated technology is involved, generating evidence that is digital in nature.

The role of law enforcement agencies carrying out criminal investigation becomes even more crucial when they are tasked to collect evidence that by its very nature is intangible, requiring expert knowledge and technical knowhow. This has necessitated the development of a new branch of forensic science, called computer forensics or digital forensics. In technical terms, computer or digital forensics can be defined as the process of identification, acquisition, preservation, analysis, and documentation of any digital evidence. The objective of digital forensics is to establish whether a crime has been committed or not by carrying out criminal investigation of digital evidence, while preserving such evidence in its most original form. According to US department of Justice, it includes formalised and approved methodology to:

a. Collect
b. Analyse and
c. Present data in a court of law.

In the criminal justice system of India, the field of digital forensics is relatively new and still in the developmental stage. As such, it is plagued by many obstacles and shortcomings. One of the major issues faced by law enforcement agencies is their use of unscientific or outdated methods of investigation which results in the collection of insufficient data, thus leading to a higher acquittal rate, especially in case of digital crimes. The perpetrators of cyber-crimes, be it entirely in the cyber world or as an aid to traditional crimes, use advanced and sophisticated technology. Presently, the police personnel remain ill-equipped and untrained to investigate cyber-crimes or handle investigations involving computer technology and electronic evidence. In the face of advanced technology and investigations requiring sophisticated methods, they remain dependent on external forensic laboratories as well as private investigators.

In its 239th report (2012), the Law Commission of India expressly pointed out that law enforcement agencies in the country are not only understaffed, but also suffer from lack of forensic as well as cyber experts in their departments. Furthermore, there are few forensic science laboratories that can aid investigating officials in a timely manner. Thus, the investigative officials end up leaning more towards gathering oral evidence than gathering scientific and digital evidence. This affects the quality of evidence gathered and the entire criminal investigation.

The lack of consistent forensic procedures regarding search and preservation of electronic evidence further leads to discrepancies in the handling of such evidence by the authorities. Different law enforcement agencies create their own manuals or guidelines for collecting electronic evidence, resulting in a system-wide disparity between the methods and type of evidence gathered. Additionally, forensic experts in India lack awareness regarding evidentiary rules and are not adequately trained to collect or extract admissible electronic evidence, affecting the admissibility of such evidence in the courts.

Law enforcement agencies are the first responders to a crime. It is they who first encounter the evidence at a crime scene. As such, their role in the criminal justice system cannot be overlooked. It is thus important to address the challenges faced by them during investigation, with special regard to digital forensics. The objective of this paper is to understand the difficulties faced by law enforcement agencies in India while dealing with digital forensics and handling electronic evidence. It will be supported by both qualitative (existing literature) and quantitative (interviews and questionnaires) data gathered from relevant professionals in the field. Possible solutions and suggestions will be put forward, based on an analysis of the data so gathered.

2. PRESENT SCENARIO IN INDIA:

As per the report published by the National Crime Record Bureau (hereinafter referred as "NCRB") in 2021 the total number of computer related crime cases registered all over India are of 52,974 showing an increase of 5.9% in 2020 (50,035) and the rate of crime under this category further increased from 3.7% in 2020 to 3.9% in 2021. There has been an major increase in the number of computer related crimes or cybercrimes in Delhi NCT in the following years:

Year	No. of Cyber-crime cases registered
2019	115
2020	168
2021	356

As of June 2023, the cyber-crimes registered in Delhi increased to 200% as compared to the same period in the previous year. Over 24,000 computer related offences have been registered till June 2023 whereas only 7500 were received by the Delhi Police in 2022.

With the advancement of science and technology, the cases have consequently been rising. The nature of the crime also has become really technical and highly sophisticated in nature. Due to this rise, there are many challenges faced by the law enforcement agencies in India, who are the nodal points in the entire criminal investigation process, right from the collection of the evidence till they are produced before the court. The law enforcement agencies play a more important role when gathering intangible evidence and it requires technical expertise to deal with the electronic evidence. There have been instances where the agencies have not complied with the law and rules of handling electronic evidence, and thus, making the evidence unreliable and in some cases, inadmissible.

Police personnel in the traditional as well as the cyber police stations have expressed their helplessness while dealing with the computer related crimes and cyber-crimes due to various reasons, such as lack of expertise, not being properly trained, non updation of available technology, etc. Cyber-crimes require a highly sophisticated investigation process and the present procedure is not adequate. It needs to be amended, so as to not only be able to meet the needs of the present, but to also be future-proof without regular upgradation.

The 239th Law Commission Report (2012) identified the poor quality of investigation by police as one of the main reasons for the low conviction rate of crime in India. This observation is further supported by the recent report of NCRB in 2021 which suggests that the conviction rate under computer related crime under Indian Penal code was only 38.1% and under the IT act was 44.7%. The reason for this gap is that our police personnels, who are the most significant part of our criminal justice system, do not have proper training and expertise to meet the changing demand of the investigation process. The criminals are now using the most advanced technology to commit crimes. They are
far ahead of our law enforcement agencies. To catch the criminals and stop crimes, the agencies need to have:

A. Proper training and expertise to understand the changing dynamics of crime and criminals.
B. Proper resources and access to advanced technologies, along with upgraded existing tools in the police stations as well as in the forensic laboratories.
C. Proper rules for the collection, analysis, and preservation of the electronic evidence.
D. A standardised and uniform procedure for handling electronic evidence.
E. Proper training and tools to overcome the digital forensic challenges faced by them.

There are a lot of challenges faced by the police personnels and other law enforcement agencies in their day-to-day life. Considering these deficiencies, the Second Administrative Reforms Commission (2007) recommended that the states should have proper investigative units to investigate criminal offences within the police force so as to conduct better investigation of crimes.

There have been various instances where the law enforcement agencies have found to be ill equipped and untrained to collect, handle, and preserve electronic evidence. In one of the instances, in a laptop theft case, there was no effort made by the IO to put MAC address on surveillance. In similar cases, police personnel rarely put the International Mobile Station Equipment Number (IMSE) to use for tracking stolen mobiles. Even trial courts have raised this concern and asked the top police officials to provide training to the officials at the level of constables and head constables, as these officials are the main personnel who go to the field for investigation of a crime. The courts also stressed upon the poor knowledge of the electronic and forensic techniques which result in collection of poor quality of evidence, which ultimately affects the investigation process, with the ultimate casualty being the administration of justice.

In the absence of a standardised computer forensic procedure in India, the problem of collecting, or seizing inadequate electronic information can never be resolved and will increase with the advancement of technology.

Collection and investigation of digital evidence from computers is a challenging job for the police and for the other investigating agencies involved. It requires technical skill and expertise and it is unfortunate to note that law enforcement agencies in India are found to be severely wanting. Electronic evidence is not visible to the eyes and is not tangible evidence, unlike physical evidence. It requires special skills and expertise in handling digital evidence for the investigation of cyber-crimes. Therefore, collection of this evidence requires a working knowledge of the law, as well as forensics to interpret such evidence.

Another major issue faced by our law enforcement agencies is one of Jurisdiction. The legal principles relating to the investigation of cyber-crimes and crimes related to the computer vary across jurisdictions. In today's world of internet and computer networks, crime can be committed from anywhere in the country and the world. But due to the non-uniformity of procedure nationally and internationally, proper investigation is a
major problem. However, to bring uniformity in the investigation process there are a few international standards that have evolved over a period. These standards specify a clear method and procedure in the form of a published document. However, jurisdictional issues remain a problem even when the investigation involves inter-state evidence collection within

the country itself. There are no clear protocols or rules for collection of digital evidence in this respect.

The field of computer forensics, which combines law and computer technology to investigate crimes, has just arisen. The original electronic record is duplicated by the forensic professionals, who also preserve, examine, and present the copies to the courts. The key role in this process is played by the law enforcement agencies who are the first responders in handling the electronic or digital evidence related to any crime. In light of this, it is crucial to address the difficulties that the law enforcement agencies face throughout this procedure, so as to ensure that the rules of evidence are met when such evidence is presented to the courts. Since the evidence presented in the court is a copy, it is only relevant and admissible if it is a faithful reproduction of the original.

3. GROWING IMPORTANCE OF ELECTRONIC EVIDENCE: THE ROLE OF COMPUTER FORENSICS

The use of science in forensics is to investigate cases of crime and establish the facts. Both medical (such as blood and DNA) and physical evidence (for example, tire tracks and bullets) are widely accepted in courts as well as in the hearts and minds of the public and the law enforcement community. The function of computer forensics and digital investigations is significantly less well recognized and understood.

The Internet history, cache, automatic Word backup files, deleted files, Metadata, and registry entries are just a few of the things that might leave a trail of activity after using a computer or network. Instant chat logs and email headers can provide information about the intermediary servers that information has passed through. Every computer system that accesses a website is listed in the server logs. The exception being zero logging services.

Rapid changes are a constant in the field of information technology, resulting in an increase in usage of cyberspace which ultimately results in increase in cyber-crimes. The growing reliance on electronic communication leads to the misuse of the information available in cyberspace. These electronic components form up the electronic evidence in the courts.

Digital or electronic evidence is not limited to personal computers, or digital devices as is commonly understood. It is found in the form of emails, digital photographs, ATM transaction logs, whatsapp chats, social media profiles, documents, internet browser histories database, compact discs, DVDs, Global Positioning System Tracks, digital camera, memory sticks, and memory/ SIM cards, cell phones, etc. Such electronic evidence is voluminous, easily modified, easily duplicated, and more difficult to destroy.

There is an increasing reliance on the new scientific means of investigation i.e., computer forensics, for extracting the evidence from computers and computer systems, to aid in securing a conviction. Computer forensics, also known as “Digital Evidence” is an emerging area of forensic science dealing with the evidence found in computers and other electronic devices[iii]. It is an integration of law and computer science which helps in the investigation of crime as it is concerned with the identification, extraction, and analysis of digital data. It extracts data which otherwise could not be recovered such as deleted texts, images or access to files containing documents.

It is very important that the investigation agencies comply with a legal procedure while dealing with the collection, preserving, and analysis of the computer or electronic evidence. The present laws in India fail to contemplate the computer forensics techniques used to assess the computer systems. The lack of adequate mechanism to appreciate the computer-based evidence has resulted in poor admissibility of the evidence in the court of law. The lack of clarity over the legal procedure with respect to the collection, preserving and analysis of the electronic evidence ultimately leads to hurdles in utilising the computer forensic procedure during criminal investigation and acquitting of the accused person.[iv]

4. INVESTIGATION OF COMPUTER RELATED CRIMES AND HANDLING OF ELECTRONIC EVIDENCE

A. Role of Investigations in Criminal Proceedings

In the administration of criminal justice, investigations play a pivotal role. The primary objective of the criminal justice system is to provide justice for all parties, including the accused, the victim of the crime, and society. The acquittal and conviction of an accused person in a criminal case depends on the investigation procedure to a great extent. There is a great responsibility on the investigative team to fulfil their duty to leave no stone unturned when they are investigating a crime, because people put their faith in the system and the law enforcement agencies are the most important link who ultimately lead the victim or accused to justice.

The Hon'ble Supreme Court of India in *Jamuna Chaudhary and others vs state of Bihar AIR 1974 SC 1822* held:

"The duty of an investigating officer is merely not just to ensure the bolstering up of a prosecution case with appropriate evidence which may enable the Court when it comes to the process of recording a conviction but rather it should also be concerned while it comes to bringing out real and unvarnished truth."

In the matter of *H.N. Rishbud and Inder Singh v. State of Delhi, 1955 AIR 196* the Hon'ble Supreme Court of India while laying down the investigative procedure, exhaustively held:

"...under the Code investigation consists generally of the following steps:(1) Proceeding to the spot, (2) Ascertainment of the facts and circumstances of the case, (3) Discovery and arrest of the suspected offender, (4) Collection of evidence relating to the commission of the offense which may consist of (a) the examination of various persons (including the accused) and the reduction of their statements into writing, if the officer thinks fit, (b) the search of places of seizure of things considered necessary for the investigation and to be produced at the trial, and (5) Formation of the opinion as to whether on the material collected there is a case to place the accused before a Magistrate for trial and if so taking the necessary steps for the same by the filing of a charge sheet under Section 173."

In the case of *Sidhartha Vashisht @ Manu Sharma v. State (NCT of Delhi) AIR 2010 SC 2352* , the Supreme Court of India established the principle of a fair investigation and trial, ruling that the investigation must be "judicious, fair, transparent, and expeditious" to ensure adherence to the fundamental principles of the law.

The lack of technical equipment to carry out the investigation frequently prevents the investigating authorities from conducting efficient investigations. Due to the dearth of forensic science laboratories and the fact that recent crimes have become increasingly technically difficult to solve, forensic experts have been unable to provide the investigating agency with timely help. As a result, the police rely more on oral testimony than on scientific and circumstantial evidence, which would have been more important in drawing a reasonable conclusion[v].

B. Investigation in Computer- related Crimes

In today's time, the crimes are not just limited to their traditional way, rather with the innovation of computers and the internet now we see crimes related to computers and cybercrimes. The traditional procedural laws i.e., Code of Criminal Procedure, 1973 (hereinafter referred as "CRPC '') fails to adequately address computer related crimes. It does not clearly specify the procedure and manner to investigate and collect the electronic evidence and evidence involving computer related crimes and other electronic devices.

Computer related crimes require adequate technical expertise for investigation. It requires ample knowledge and skills which facilitate a proper investigation. The investigative team or agencies have to be well equipped and trained to do an effective, fair and transparent investigation.

In India, the Information Technology Act, 2000 sets up a special procedure for investigation of crimes involving computer and cyber-crimes. The provisions of this Act clearly specifies that the investigation of the cyber-crimes must be conducted by the inspector. The power to investigate lies with an inspector level officer. However, based on the pilot study done by the researchers, it was found that in reality, we never see an inspector investigating the crime on ground, rather it is a constable or sub-constables or sub-inspectors who conduct the investigation. These officials lack the requisite skills needed which may be in terms of education, skills, training and experiences.

The changing trends need every official to be well versed with the fundamentals of computer forensic procedure as it plays an important role in the identification, collection and preservation of electronic evidence. Each time a crime involving computers occurs, the investigators must be able to establish a connection between the crime and the computer used, follow all legal procedures to search and seize the computer used in the crime, and collect electronic evidence. Likewise, it is the duty of judges and prosecutors to be aware of the role of electronic evidence in criminal investigations.

It is important to note that in a recent development in some states, especially in Delhi, cyber cells have been converted to cyber police stations which have the requisite technical equipment to extract and preserve the electronic evidences and also have the trained staff to work on electronic evidences. It is pertinent to mention that in Delhi police has established cyber police stations in each of the 15 districts and now the total goes to 15 cyber police stations in Delhi itself.

During the pilot study conducted by the researchers involving the traditional as well as cyber police stations of various districts, it was found that despite having cyber police stations, their staff still need to take help from forensic laboratories since the training provided to the staff of these police stations is very basic. To deal with technically advanced evidence, help is sought from NCFL, Dwarka. There is a huge gap between the technology, which is advancing day by day, being used to commit crimes and the skills needed to identify the electronic evidence in such cases.

C. Handling of Electronic Evidence and Law Enforcement Agencies

Forensic investigation is the utmost important step in identifying and bringing to justice a possible criminal act. It tests the ability of an investigator to identify the potential and important evidence available at the crime scene. It is a proper investigation which leads the victim to justice. In case of computer related crimes, electronic devices such as computers, mobile phones etc. may not be directly connected with the crime scene, yet they may provide leading information to the crime committed.

The foundation of a digital investigation, which entails the stages of preparation, collection, and preservation of electronic evidence, is laid by the effective handling of computers and networks as evidence linked to a crime. A digital investigation can be severely hindered by lack of integrity at the early crime handling stage, by omitting important details or failing to properly preserve digital evidence, making it inadmissible in court. However, a well-established process for handling evidence might not be able to account for every difficulty and circumstance that arises.

When creating policies and procedures for addressing computer-related crime scenes, it is crucial to keep in mind that the legal principles governing such investigation processes differ among jurisdictions. In order to bring uniformity to the investigation of crimes using computers, it is important to note that there are worldwide standards that have developed over time. A standard is a written document that outlines accepted specifications and practices to guarantee that a material, product, process, or service is suitable for its intended use and functions. It is an agreement that deals with issues pertaining to security, dependability, and effectiveness (ISO 2009), among other things. The development of international standards is a crucial step toward achieving consistency in findings and mutual compliance across geographical and jurisdictional boundaries.

The pilot study results reveal that in India there are no uniform guidelines regarding digital forensic investigation, so we follow ISO: 27037:2012, which is a standard set by the International Organization for Standardization (ISO) providing guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value.

D. Search and Seizure

In every investigation process the collection of material information and evidence is done through the search and seizure. The search and seizure process is more technical in nature for cybercrimes and computer related crimes than the traditional crimes. A court-issued warrant gives the police a limited ability to invade a citizen's privacy. It is vital to note that search warrants are crucial tools for carrying out operations of search and seizure. To search cyberspace and seize electronic evidence in the case of computer crimes, the investigating officers must get a warrant. In India, the provisions relating to search warrants in criminal law are issued under Section 93 of the Code of Criminal Procedure, 1973, which stipulates that a judicial officer may issue a search warrant on the basis of reasonable grounds as specified in the provision and may specify the location or type of document to be searched.

When it comes to the scope of the data to be searched, cybercrime searches are more challenging and problematic. Investigators may stumble onto damning data while looking into a computer-related crime among thousands of unrelated files that are virtually impossible to distinguish at the search site. This has caused a serious dilemma as computers retain a significant quantity of information, and because that information is very technical in nature, it is extremely difficult to extract even a small fraction of it as evidence to present in court.

E. Chain of Custody

One of the most crucial components of authenticity is upholding and recording the chain of custody, which ensures that the person in possession of the evidence when it is produced in court is the same person who had it when it was processed during the investigation. To put it another way, a chain of custody is a road map that shows precisely how evidence was gathered, stored and examined in order to be presented as evidence in court. Because electronic evidence can be easily corrupted, establishing a clear chain of custody is essential. The reliability of any electronic evidence used in a criminal inquiry is ensured by a transparent chain of custody. If the chain of custody is not preserved, the electronic evidence presented in court may be challenged and ruled inadmissible.

5. CHALLENGES IN HANDLING ELECTRONIC EVIDENCE

Because legal procedures differ from state to state, investigators handling electronic evidence find it difficult and ambiguous to determine the appropriate course of action. Certain states have implemented extremely strict policies concerning searches conducted without a warrant. The court concluded in United States v. Park that a warrantless mobile phone search is unnecessary and inappropriate because cell phones can store more data than pagers and are therefore less likely to have their contents lost.
In the same way, the court held in United States v. Wall65 that "looking through data saved on a mobile device is comparable to looking through a confidential correspondence." It happens frequently that the investigators obtain a search warrant from the court to conduct a search; yet, the evidence may not be worth presenting in court since the forensic technique did not follow the law. An improper search could be, for instance, going through unsealed mail and unseen texts or failing to properly record the chain of custody. It is now extremely difficult for investigators to conduct the investigation in an efficient manner due to jurisdictional restrictions and inconsistent legal procedures.

5.2. An Empirical Study of Cyber Police Stations and Traditional Police Station in Delhi

i. Methodology

To tackle the issues discovered after an analysis of the available literature, the researchers have combined doctrinal and empirical research methods. The research conducted spans a period of two months. Reviewing primary and secondary literature serves as the method of data collection. Six different original sources, including statutes, manuals, guidelines, and regulations, as well as related legal papers and court rulings, have received special attention. Along with using a doctrinal approach, the researchers have also conducted a pilot study to comprehend the many steps involved in digital forensics about handling of electronic evidence by law enforcement agencies and the courts. To gain a deeper understanding of the computer forensic methods used by various agencies in particular circumstances, the researchers have also conducted interviews as part of the pilot field study to understand the challenges possessed by the law enforcement agencies in identifying, collecting, and preserving the electronic evidences collected during the criminal investigation of traditional crimes as well as cyber-crimes. A total of ten police stations in the National Capital Territory (NCT) of Delhi were studied. The respondents were further subdivided into traditional police stations and cyber police stations, owing to the specialised nature of the latter in dealing with cyber-crimes. Informed consent of the participants was sought for the study. All respondents were of the Sub-Inspector (S.I.) level. The responses were then thematically analysed to arrive at the findings of the survey. The goal of this study was to examine the newly emerging field of computer forensics from a techno-legal perspective and evaluate the ground level difficulties faced by the police personnels undertaking digital forensics during investigation of a crime scene, which ultimately impact the admissibility of electronic evidence so collected, in the criminal justice system.

ii. Results

A pilot study was undertaken of 10 police stations in the National Capital Territory of Delhi, which were further sub-divided equally into traditional police stations and cyber police stations. The following challenges emerged with regards to the challenges faced by them during investigation of crimes related to computers:

Qualifications of staff handling electronic evidence.

The study sought to grasp the educational qualifications that are deemed necessary to handle electronic evidence in the field of digital forensics. The results indicate that there are no specific educational qualifications or criteria that a person must fulfil in order to handle digital evidence. In most instances, graduation from any field was enough.

Digital forensic tools and level of training of respondents.

One of the main questions that the study attempted to answer was how equipped the respondents are to handle digital crimes and electronic evidence, both in terms of the tools available to them as well as their level of training. While use of technology and computer systems affect crimes in both the traditional physical space as well as cyber space, a distinction has been made with regards to traditional police stations and cyber police stations owing to the specialised nature of the latter in dealing with cyber-crimes.

Questions	Traditional police stations	Cyber police stations
i. Do you feel that the police personnels are well equipped and trained for handling investigations involving computers or crime related to electronic devices?	The present staff is not at all well equipped to handle even the basic electronic evidences	Presently, they are trained and equipped to handle electronic evidence to a certain extent.
ii. Is there any special training provided to the staff to deal with highly sophisticated and technology advanced crime committed to the staff?	While some respondents claimed that such training is provided only to the higher officials, others stated that they do receive basic training from time to time but it is insufficient.	Basic training is generally provided to the staff from time to time but dealing with advanced crimes and evidence require professional/ outside help.

The above sample results show that both traditional and cyber police stations are not adequately equipped to handle crimes involving electronic devices. Moreover, the training provided to them is not enough to handle electronic evidence. They still need to seek help from forensic labs such as National Cyber Forensic Laboratory (NCFL) or third- party experts to address issues of digital forensics.

Forensic experts

The study attempted to find out if the police stations have any forensic expert(s) as a part of their investigating team. Respondents from traditional police stations denied having any such forensic expert(s) in their investigation teams. This makes it very difficult for them to carry out digital forensics in a crime scene that involves the use of computer systems.

On the other hand, respondents from cyber police stations stated that they do have forensic expert(s) as part of their investigation teams. However, there is a discrepancy in their level of expertise. While forensic labs in some cyber police stations are equipped to handle preliminary digital forensics on their own, others are equipped to only handle digital forensics at the basic level or extracting evidence in a limited manner. For other devices or a more advanced analysis, they are dependent on NCFL, Dwarka.

Guidelines or manual for digital forensic investigation in India.

Another important objective of the study was to assess whether there exists any guideline or manual that works as Standard Operating Procedure for digital forensic investigation in India. Respondents were further asked what procedure they follow while carrying out digital forensic investigation.

There was an unanimous agreement that no standardisation exists in India for digital forensic investigation. The procedure most commonly followed is the one set by the International Organization for Standardization (ISO), which provides guidelines for identifying, collecting, acquiring and preserving digital evidence.

Challenges faced during extraction of electronic evidence.

Respondents were asked about the challenges that they face in extracting electronic evidence during investigation.

Traditional police stations	Cyber police stations
• Lack of technical knowledge or expertise. • Lack of consistent guidelines for collection, acquisition and presentation of electronic evidence. • Rapid change in technology. • Immensity of data in the current age. • Use of anti-forensic techniques by criminals.	• Advancement of technology. • Ambiguity of criminal and evidentiary rules and lack of a consistent guideline/manual for digital forensics. • Non-updation of existing Criminal Law and Evidence Law to include digital crimes and digital forensics. • Jurisdictional issues with – a. Interstate investigation b. Investigation involving foreign s states.

Need for specific law or rules regarding digital forensics.

Finally, the study attempted to determine if respondents felt the need for a law that specifically deals with investigation involving digital forensics, keeping in mind the needs of the country. All respondents agreed that formulation of either a uniform set of rules/guidelines or a specific law regarding handling of electronic evidence is necessary. It will bring uniformity and clarity to digital forensic investigation and lead to better admissibility of electronic evidence in the criminal justice system.

5.3. Findings and Analysis

The study revealed many shortcomings that exist in the processing of digital evidence carried out by law enforcement agencies. Broadly, these shortcomings can be highlighted as follows:

Resource constraints- lack of adequate resources is one of the primary hurdles faced by law enforcement agencies during an investigation involving digital forensics. Police stations are not equipped with the latest tools and methods that are required to investigate crimes which use advanced technical knowledge of computers. Moreover, such resource constraints are not only limited to the quality and quantity of equipment, but also include financial constraints. Since the presence of cyberspace has broadened the geographical horizons of crime, investigations are also required to be carried out in a large area. However, the funds allocated to the agencies are limited and often insufficient to carry out large scale investigations. This often adds to the delay in solving a crime and bringing the victims as well as perpetrators to justice, if at all.

Efficiency and strength of the staff- The level of knowledge of the existing staff in handling electronic evidence is inadequate. They are unaware of, and untrained in, the use of necessary tools and scientific methods which have emerged with the advancement of technology. Perpetrators of cybercrime use increasingly advanced ways to get away with their deeds. Many times, investigative officials are baffled when they have to investigate a computerised ecosystem. They do not know how to properly search for evidence in such an environment, thus missing out on vital clues. So long as the police personnel remain untrained, they will be helpless to deal with such crimes.

Furthermore, it was observed that the investigative agencies are vastly understated to keep up with the high rate of crimes being committed. This causes not only a delay in investigating existing crime reports, but also creates backlogs and delays in accepting new reports of crimes.

Lack of forensic experts- When the crime committed involves advanced technology, it requires the use of professional knowledge and methods to be solved. However, not every police station has a forensic expert on its team that can carry out digital forensics during investigation. This is a major issue, as acquiring and handling electronic evidence requires specialised knowledge and expertise over computer technology. Currently, even the cyber police stations do not have sufficient staff who can fully carry out digital forensics in their departments.

Jurisdictional issues- The digital era has made it possible for crimes to be committed across multiple territorial jurisdictions. Perpetrators need not be physically present at the place where the crime is being committed. This raises jurisdictional concerns for the law enforcement agency carrying out the investigation. Jurisdictional issues may arise inter-state within the territorial borders of the country itself or even with a foreign nation. Thus, a procedure has to be established for carrying out such investigations without hindering the process of justice and sovereignty. This calls for better cooperation between agencies at both the national and global level.

Lack of a Standard Operating Procedure- There is no uniform procedure for handling electronic evidence. Different agencies use their own procedures. Although the procedure set by the ISO is commonly used by investigative officers, it does not cater to the specific needs and circumstances of the country and must be supplemented with indigenous procedures. It would be beneficial to formulate a standard procedure to be followed across the country which caters to the specific needs of India.

Logistical difficulties- Law enforcement agencies suffer from issues such as lack of high-speed internet connections, insufficient storage capabilities for electronic data, lack of modern amenities for handling electronic evidence, etc.

Overburdened forensic labs- Currently, police stations are dependent on forensic labs such as National Cybercrime Forensic Laboratory (NCFL), Dwarka, for carrying out digital forensics during investigation. The number of such labs are limited. They have to handle matters from many different police stations, making them overwhelmed and unable to provide timely help, thus causing delay in the process of justice. There is a need to increase the number of such labs and set them up in every district so that they may help share the burden of law enforcement agencies.

Need for harmonizing law and policy- To tackle the issues faced by investigative agencies, it would be beneficial to have laws and policies that specifically covers matters of digital forensics in India. Such laws and policies would ensure standardisation of the process of digital forensics as well as act as a guideline on how to handle electronic evidence. The existing rules that cover digital forensics in India are scattered and not sufficient to keep up with the changing times.

5.4. Investigation Of Computer-Related Crimes: The Judicial Approach

With growing technology, the judiciary has also felt the need to acknowledge the use of tools and technology in the investigation of crimes. In a number of rulings, the courts have emphasised that the Indian Evidence Act of 1872 be followed and that technology should be used to its fullest advantage when proving a case. While upholding the significance of a thorough investigation of computer-related crimes, the judiciary has also noted that, in order to prevent improper handling and collection of digital evidence, law enforcement agencies must follow a protocol that complies with the rules of evidence during the process of identification, collection, and preservation of such evidence. Below, we explore a few court rulings that dealt with the investigation of such crimes in order to better appreciate the difficulties that were faced.

i. Vijesh v. The State of Kerala

This judgement was rendered in accordance with Section 79A of the Information Technology Act of 2000, after the notification of the Examiners of Electronic Evidence. The case provides clarification regarding the judiciary's modified strategy following notice. The Court ruled that a person who examines electronic evidence does not need to demonstrate in court that they are an expert in that particular field. As soon as the institution is informed, its expertise is established. In other instances, the expert who reviewed the electronic evidence will need to demonstrate his expertise in front of a judge. Even though the interpretation was provided by an expert in the examination of electronic evidence, it nevertheless casts doubt on the validity of the evidence.

The court is yet to set any guideline with regard to this. Additionally, the Court observed the following:

"Given the nature of evidence to be copied, maintaining the evidential continuity and integrity of the evidence that is copied is of paramount importance. Such evidence will be subjected to cross examination in relation to its integrity. In other words, the process of copying and handling such evidence should be carried out to the highest possible standards."

The Court further ruled that in situations when a mobile phone is used to commit a crime, the officer's first and foremost responsibility is to protect the device to avoid data loss or manipulation. He should have taken a picture, documented any information on the screen, and then logged the present condition of the equipment. If the gadget was on, it ought to have been turned off, and the batteries ought to have been taken out. The different data, metadata, and call records would all be preserved if the phone was turned off. It would also stop any attempts to remotely delete the contents of the phone.

Furthermore, the officer was required to confiscate any cables, chargers, packaging, manuals, etc. to aid in the investigation and reduce the time needed for any inspection by the digital evidence specialist. The owner of the phone had to be asked for the device's password or pin, in case it had one. The phone needed to be sealed in antistatic packaging like a plastic bag, envelope, or cardboard box prior to forwarding to the digital evidence expert along with the gathered data. Only the specified professional is able to acquire, copy, and analyse the digital evidence.

The Court observed that none of these procedures were adopted by the investigating officer, and concluded:

"It is high-time for the State Police to bring out a good practise guide for digital evidence, if they intend to tackle cybercrime head on. The cyber criminals are way ahead of the law enforcement officers and urgent measures are to be taken to train officers to successfully prosecute the offenders. Flaws committed by the officers, such as in the instant case, may prove fatal to the prosecution. Officers, who are engaged in investigation of cybercrimes, are required to be

trained in best practices to tackle the criminal misuse of current and emerging technologies." (Para 9)

ii. Abdul Rahaman Kunji v. State of West Bengal

Highlighting on the need for competent officers in cyber police stations, the Court held the following:

"With the rise in crimes involving electronic communications, whether by using the Ethernet, Wi-Fi connections or mobile networks, we are of the opinion that a competent officer from the Cyber Police Station must be inducted mandatorily into the investigating team immediately if such a case arises. This would ensure that the originator of the electronic communication is nabbed swiftly and appropriate evidence is collected and led to prove the e- 76 (2015) 1 Cal LT 318 178 mails, telephone calls, or electronic messages during trial of the case. In cases such as the present one it would be more useful perhaps in future for the prosecution to pursue leads from the Internet Protocol (IP) address from which the mails are sent. This would provide the exact location of the computer or smartphone or other devices from where the mails are sent. Thus, even if an email or electronic communication were to be sent from a computer in a cybercafé, a coffee shop or any location where a local area network (LAN), Wi-Fi (wireless fidelity) connection or mobile network is available it would be possible to identify the originator.

Today, closed circuit television cameras are being installed in most areas where computers are accessible or where it is possible to use one's own devices which access Wi-Fi connections, or mobile networks, e.g, personal computers, mobile phones, tablet computers etc. The evidence obtained from such video recordings could be used to corroborate the identity of the originator of the electronic communications who sends such communications especially from a closed area. This would make it easier for the investigating officers in future to unearth the truth in crimes involving electronic messaging and communications with more certainty. It is necessary for the investigation agencies to keep pace with the technological advances in the world of electronics and to prove their case in accordance with the Evidence Act by making the best use of such technologies." (Para 71)

iii. Dilipkumar Tulsidas Shah v. UOI

Dilipkumar Tulsidas Shah, the petitioner in this case, approached the Supreme Court of India with a Public Interest Litigation (PIL) in accordance with Article 32 read with Articles 14, 19, and 21 of the Indian Constitution. In order to provide laws, regulations, and guidelines for a successful investigation of cybercrime, the court was petitioned for assistance. The petitioner further emphasized how the current system of cybercrime investigation lacks procedural safeguards, which results in harassment of citizens. The petitioner noted that one of the shortcomings of such an inquiry was the employment of traditional techniques to combat cybercrime. The petitioner requested that the Apex Court issue a writ of mandamus ordering the government to educate the judiciary, internet service providers, and investigating agencies about the various types of cybercrime recognized under the 2008 amendment to the Information Technology Act of 2000.

iv. Prof. K.G.Varghese v. State Of Kerala

The case at hand concerns the online distribution of defamatory materials directed at the petitioner. The petitioner's complaint was that the case's investigation was not being handled in a satisfactory or effective manner. Any person who brings a complaint to court must be satisfied that his complaint was treated as property at the end of the day. The Court ruled that the Police must ensure a free and fair inquiry is conducted by a qualified officer, particularly in a case like this that involves a cybercrime. The investigative procedure will not be satisfactory at all if it is carried out by an officer who is unfamiliar with the complexities and technical components of such crimes.

v. State of Punjab v Amritsar Beverages Ltd

In this case, the Court referred to the difficulties of enforcement officers which may be faced by them who may not have any scientific expertise to tackle the new digital evidence. The Court held:

"Internet and other information technologies brought with them issues which were not foreseen by law as for example, problems in determining statutory liabilities. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or did not have the sufficient insight to tackle the new situation. Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus. Information Technology Act, 2000 although was amended to include various kinds of cybercrimes and the punishments therefore, does not deal with all problems which are faced by the officers enforcing the said Act."

vi. Arjun Panditrao Khotkar v. Kailash Kushnrao and Ors.

The question before the Supreme Court of India was whether an electronic record containing an electronic signature could be admitted as secondary evidence under Section 62 of the Indian Evidence Act, 1872, in the absence of the original document. The electronic record in question was a voice recording of a conversation between the parties, which was submitted as evidence in a civil suit. The court held that an electronic record containing an electronic signature could be admitted as secondary evidence under Section 62 of the Indian Evidence Act, 1872, in the absence of the original document, provided that certain conditions were met. The court stated that the authenticity of the electronic record must be proved in the same manner as any other electronic record under Section 65B(4) of the Indian Evidence Act, which requires a certificate to be produced by the person who has produced the electronic record.

The court further held that the requirement of a certificate under Section 65B(4) of the Indian Evidence Act could not be dispensed with, and that the certificate must accompany the electronic record when it is produced in court. The court also clarified that the certificate must be issued by a person occupying a responsible official position
in relation to the operation of the relevant device or the management of the relevant activities, and that the person must state that the electronic record was produced during the ordinary course of such activities.

The Supreme Court of India has taken a pragmatic and nuanced approach towards electronic evidence, recognizing both its potential benefits and its potential pitfalls. The Court has emphasized the need for careful evaluation of electronic evidence on a case- by-case basis, and has recognized the importance of authenticity, integrity, and specialised knowledge in dealing with such evidence.

As a result of the analysis of cases involving electronic evidence done above, the judiciary has begun to acknowledge that handling electronic evidence has been difficult for law enforcement agencies and that it has characteristics that set it apart from other types of evidence. The courts have also acknowledged the need for extreme care and caution when handling electronic evidence in order to prevent any manipulation or tampering that would compromise the validity of the evidence itself. Any improper treatment of digital evidence shouldn't result in any bias against the accused.

6. RECENT DEVELOPMENTS IN THE FIELD OF COMPUTER FORENSICS AND ELECTRONIC EVIDENCE

6.1. New Criminal Law Bill

On August 11, 2023 three new Bills were proposed to be discussed in the Houses of Parliament to replace the Indian Penal Code, 1860 ("IPC"), the Code of Criminal Procedure, 1973 ("CrPC"), and the Indian Evidence Act ("IEA"), they are the Bharatiya Nyaya Sanhita, 2023 ("BNS"), Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"), and Bharatiya Sakshya Bill, 2023 ("BSB"), respectively. The new criminal bills were submitted on the justification that the old laws were antiquated, unnecessary, and unable to keep up with the demands of our society, which is always advancing toward various breakthroughs, particularly in artificial intelligence and technological developments. Few of the changes are as follows:

- The BNSS Bill provides under Clause 176(3) forensic investigations for offences carrying a minimum seven-year jail sentence. In these situations, forensic professionals will go to the crime scene to gather forensic evidence while also documenting the event on a cell phone or other electronic device. If a state does not have its own forensics centre, it must use one in another state. This step will strengthen the investigation process and will also help in identification and collection of effective electronic evidence for the further process.
- Under section 105 that search and seizure shall be recorded through any audio-video electronic means preferably cell phone and the police officer shall without delay forward such recording to the concerned authority. Increased use of electronic evidence and forensics during investigation. By this step, the changes of false cases as well as the process of computer forensics will be ensured during the investigation of the computer related crimes i.e. identification, collection and preservation of the electronic evidence.
- BSB makes electronic or digital records admissible as evidence, thereby they will have the same legal effect as paper documents.

6.2. Other Developments by the Government

As the first institution of its kind in the nation to use this technology, the Delhi Forensic Science Laboratory (DFSL) and the Delhi Police will now use blockchain technology as part of their e-forensic application to create an irrevocable and transparent record of the chain of custody for evidence. The technology will have "unlimited capacity and storage for an infinite time period. It will also ensure unbiasedness as well as transparency in the process.

7. CONCLUSION

As society progresses on the path of scientific development and technological advancements, there will inevitably be changes in the way crimes are committed. The criminal justice system needs to adapt to these changes to remain effective in maintaining law and order and solving crimes. The new dynamics that have been added to crime- both in the traditional physical space as well as cyber space, necessitate the use of the latest tools and technology to carry out digital forensics during an investigation.

The state of digital forensics in India is still at the developmental stage. Thus, it is still plagued by many obstacles and shortcomings. The use of unscientific or outdated methods of investigation results in the collection of insufficient data for conviction of criminals, especially when they use advanced computer systems and technological knowledge in the commission of crimes. Moreover, the police personnel remain untrained and ill-equipped to investigate cybercrimes or handle investigations involving computer technology and electronic evidence. Even in the case of cyber police stations, which have been set up specifically to handle digital crimes, the level of training to handle electronic evidence and carry out digital forensics remains inadequate. They need the aid of forensic laboratories such as National Cyber Forensic Laboratory (NCFL) or third-party experts to address issues of digital forensics, when the investigation requires knowledge of advanced methods and tools.

Furthermore, the issue of non-standardization of forensic procedures regarding digital forensics, especially with regards to search and preservation of electronic evidence, leads to discrepancies in the handling of such evidence by the authorities. Different investigative agencies create their own manuals or guidelines for collecting electronic evidence, resulting in a system-wide disparity between the methods and type of evidence gathered. This brings about non-uniformity in criminal investigation across different investigative authorities and inevitably, the criminal justice system of India. Although most investigative authorities follow the procedure set by the ISO for identifying, collecting, acquiring and preserving electronic evidence, it is still not uniform and neither is it made keeping the needs of India in mind.
Additionally, forensic experts in India lack awareness regarding evidentiary rules and are not adequately trained to collect or extract admissible electronic evidence, affecting the admissibility of such evidence in the courts. No specific qualifications have been set for selection of the staff responsible for carrying out digital forensics and handling electronic evidence. A mere graduation in any field is deemed enough. The training provided to such staff also leaves much to be desired.

There are also instances of jurisdictional issues during interstate investigations or cross border investigations involving foreign nations. This stems from the very nature of digital crimes, which allows the perpetrators to commit crimes from any part of the world without having to be physically present at the place where the crime is being committed. A procedure has to be established for carrying out such investigations without hindering the process of justice and sovereignty. This calls for better cooperation between agencies at both the national and global level.

Thus, a need is felt for either the formulation of a uniform set of rules/guidelines or a specific law regarding handling of electronic evidence, keeping in mind the special circumstances and needs of the country. Such a law, guideline or manual should include mandatory provisions for training as well as necessary qualifications of the staff handling electronic evidence. It will bring uniformity and clarity to digital forensic investigation and lead to better admissibility of electronic evidence in the criminal justice system.

8. SUGGESTIONS

After extensive analysis of the available literature as well as the observations made during the survey, the researchers present the following suggestions:

8.1. Updation of tools and technology: The tools and technology being used by investigative authorities during a criminal investigation needs to be updated. They should be provided with the latest equipment and scientific methods available in the field of digital forensics, so that they can carry out investigations of crimes that involve advanced technology. High speed internet connections should be made available to them to prevent delays. Additionally, an agreement can be reached with the mobile or software development companies that they will provide patches related to outdated technology so the investigative authorities and forensic experts can easily analyse and preserve data for evidence purposes.

8.2. Training of staff: The staff responsible for digital forensics during a criminal investigation must be properly trained. Such training is required at two levels-

i) With regard to equipment and methods- Merely equipping the investigative authorities with the latest tools and technology will not be helpful, if they do not know how to make full use of them. They should be provided with periodic training programs on the handling of new tools and methods of scientific and digital investigation. Furthermore, they should be provided with instruction manuals regarding the use and handling of such tools and technology to prevent any hiccups when using them.

ii) With regard to handling electronic evidence- Police personnel and forensic experts should be given proper training on how to handle electronic evidence, including their identification, collection, acquisition and preservation. A criteria should be set regarding the qualifications of any staff who handles electronic evidence. Individuals from a scientific or technology background would have a better understanding and knowledge of the tools and methods required for digital forensics, making them a better candidate for handling electronic evidence. Such training should be provided on a periodic basis so that they remain updated with the changing dynamics of crime and technology.

8.3. Including forensic experts in departments: Currently the law enforcement agencies across the country suffer from a lack of forensic and cyber experts in their departments. This leads to a dependency on forensic laboratories and private investigators. Instead of being tied down by such factors, it would be beneficial for police departments to have their own forensic and cyber experts who are capable of handling digital forensics at the departmental level itself. Police stations can set up cyber forensic labs within their own departments and install the necessary equipment.

8.4. Increasing the number of forensic labs: The number of cyber forensic laboratories that are available to provide aid to law enforcement agencies is also limited, making them overwhelmed with matters and causing further delay in investigation. More forensic labs can also be set up in every district so that they may help share the burden of law enforcement agencies.

8.5. Standardisation of procedure and need for a law: The procedure regarding digital forensics needs to be standardised. Most helpful in this aspect would be to have a law that specifically deals with digital forensics in India. In case such a law is unfeasible, a guideline or manual for handling electronic evidence and carrying out digital forensics should be formulated, at the very least. Not only will it bring uniformity and clarity to digital forensic investigation but also, it will lead to better admissibility of electronic evidence in the courts.

8.6. Awareness of rules: Currently, electronic evidence gathered during criminal investigation is covered by the rules stated in the Information Technology Act, 2000, the Indian Evidence Act, 1872, the Indian Penal Code (IPC), 1860 and the Code of Criminal Procedure (CrPC), 1973. However, forensic experts involved in the handling of electronic evidence are not always aware of the rules that determine the admissibility of such evidence in courts. As such, there are instances when electronic evidence gathered during investigations are deemed inadmissible during judicial proceedings, leading to acquittals of criminals or dismissals of cases. Hence, it is imperative to ensure that personnel involved in the handling of electronic evidence are well aware of evidentiary rules. Such awareness can be brought on by conducting workshops and training programs for them by those well versed with the law.

8.7. Due diligence: Investigation of a crime scene is the first step in any criminal procedure. As such it is crucial that investigative authorities maintain due diligence during any criminal investigation. More care is needed when the crime committed involves use of advanced technology. Criminal investigations are always tricky and digital forensics makes it trickier. Police personnel must maintain a keen attention to detail during investigation and collection of evidence, including electronic evidence. They must know how to conduct proper

searches in a digital environment and not miss out vital evidence due to carelessness.

8.8. Better cooperation for intestate

investigations or cross border investigations involving foreign nations: The era of digitisation and cyberspace has blurred territorial boundaries, making it possible for a perpetrator to commit crimes in a place far away from where they are located. This leads to jurisdictional issues during investigation. As such, there is a call for better cooperation for intestate investigations or cross border investigations involving foreign nations. Full support must be provided by the government to investigative authorities in this regard, so that they may fulfil their duties without excessive formalities. A special cell or department may be set up to facilitate such cooperation at both the national and global level.

REFERENCES

[1] The author is a Ph.D. Research Scholar at Faculty of Law, Delhi University. She may be reached at counsel.sadhna@gmail.com

[2] The co-author is a Ph.D. Research Scholar at Faculty of Law, Delhi University. She may be reached at meghalidas.law@gmail.com

[3] Nina Godbole & Sunit Belapure, Cyber Security 318 (2011)

[4] Barry Chen, Computer Forensics in Criminal Investigations, Dartmouth Undergrad. J. of Sci. (2013)

[5] Malik s. Sultan, Criminal Trial & Investigations, 21 (2013)