Page 289 - 301 **DOI:** *https://doij.org/10.10000/IJLSI.111104*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 5

2021

Cybercrime and Preservation of Digital Evidence in Criminal Trials

UPASANA BORAH[1] AND UJJAINI BORTHAKUR[2]

ABSTRACT

Any electronic module produces Data that can be used as evidence in a cybercrime, security alert, or cyber-attack, yet data collection, administration, and preservation are routinely neglected. In the legal area, once information is received from devices, it is critical to keep it safe and secure from the moment it is obtained until the prosecution or inquiry is over. Digital evidence preservation is critical when determining its legality in a current trial, a future trial, an appeal, or as a repository of historical information. This study analyses concept, related projects, technologies, and legal support in digital preservation in criminal investigation institutions. A framework to maintain digital information, respect the dignity, therefore boosting acceptability, and supplemented by long-term preservation methods is the inspiration with this paper.

Keywords: *Indian Evidence Act, 1872, Crime Scene, Information Technology Act, Delhi High Court, Supreme Court.*

I. THE DANGER FROM THE INTERNET

Cybercrime is any crime committed using a computer or network. The computer might have been used to commit the crime or the intended victim. Cybercrime can compromise an individual's safety and finances.

Sensitive information is obtained or shared in many ways, both legally and unlawfully. Global cybercrime includes surveillance, money theft, as well as other cross-border crimes. Cybercrime involved in at least one country is sometimes called cyberwarfare. Hacking is the "biggest one threat confronting civilisation," according to Warren Buffet.

According to a 2014 estimate (backed by McAfee), the global economy will lose $445 billion in annual. An analysis by Cybersecurity Ventures in 2016 estimated global cybercrime damages at $billion in 2020 and $10.5 trillion by 2025. In 2012, the United States lost over $1.5 billion to internet payment card theft. In 2018, research conducted by the Center for International Studies (CSIS) in collaboration with McAfee concluded that cybercrime steals roughly 1% of global GDP, or close to $600 billion, each year. The World Economic Forum's 2020 2018 Global report verified that organized

[1] Author is a student at Student at NEF Law College, India.
[2] Author is a student at Student at NEF Law College, India.

 [ISSN 2581-9453]

cybercrime groups collaborate to commit illegal acts online while calculating their likelihood of detection and conviction in the United States is less than 1%.

II. CYBER INVESTIGATIONS IN DIFFERENT LEGAL ASPECTS

- Prosecution - Use electronic evidence in a range of offenses. Criminal prosecution includes homicide, financial fraud, drugs, embezzlement, harassment, recordkeeping, and child pornography.
- Can employ technological evidence to reveal commercial and personal documents. These are only a few instances.
- Automobile and arson insurance firms may adequately defend themselves against claims by providing electronic records of probable fraud.
- Corporations employ -This evidence to investigate probable connections between blackmail, fraud, trade secrets, and other internal and external information.
- Revenue/Enforcement/Regulation – Used in post-seizure computer asset protection.
- Counsels – They hire cyber forensic experts to handle and establish sophisticated electronic records.

III. A GUIDE TO DIGITAL EVIDENCE

Many departments are still far behind when it comes to using digital evidence to make decisions. The rapid evolution and growth of digital gadgets, economic constraints, and a lack of appropriate training opportunities are only a few reasons behind this. Computer evidence can be a significant expense, requiring permits, equipment, and a considerable time and labor investment. Securing command staff buy-in requires demonstrating a cost-effective return on investment. Funding these initiatives can be difficult for smaller agencies because it requires a combination of local, state, and federal funds. Officers can benefit from regional models and other kinds of teamwork if they know where to look for assistance. Although police training does not offer modern digital evidence training as part of their core curriculum, officers of all experience levels may contact forensic Data that can potentially influence the outcome of a case. The shortage of digital evidence extraction specialists is adding to the backlog. Because classes would pull examiners away from their jobs, a growing backlog limits training chances. It can also hinder efforts to replace outdated under technology and licenses because of financial constraints in units deemed to be underperforming.

The development of computers and digitization have been game-changing inventions for humanity. Cyberspace, like other areas of human life, has its share of risks and criminality. Diverse material and information available, easy accessibility, and broad reach have all contributed to this outcome. Despite this, the misuse of cyberspace has skyrocketed in recent years due to its widespread adoption. E-Document's legitimacy has always been a subject of debate, given how easily they may be manipulated. The legality of such digital information is a growing concern for investigat-

ors. Given that electronic evidence is more challenging to collect and interpret than conventional construction evidence, the method employed to gather and evaluate data stored on or recovered from electronic means for use in Court is critical. According to judicial precedents and legislative intent, the article analyses and investigates the admission of technological evidence in courts of law.

IV. A CRIME OF OMISSION: VIOLATION OF LAW

Digital evidence was initially used to prosecute computer crimes. With the advent of digital artifacts, practically every crime has at least one that could be used in an investigation. For that reason, digital evidence is often considered for non-computer offenses in the proactive investigation. Investigators may, for example, assume by default that suspected or victims' cloud storage account includes data, and that, if legally retrieved, such data will provide them with investigative leads.

Discovery/Accusation

Many alleged computer crimes fall just short of criminal investigation and prosecution thresholds. Increasingly, crime victims turn to the criminal justice system and forensic departments for help, so it is crucial to have protocols that help the victim capture any digital evidence or information that would be lost otherwise. There are a variety of methods for carrying out acquisitions. The method used is defined by the type the digital gadget being used. Digital evidence obtained from smartphones, such as cellphones, has different procedures than evidence obtained from computer hard drives. Evidence is retrieved from confiscated personal technology at the crime laboratory unless their live collection is used. Digital information must be collected at the forensics laboratory in a forensic context to preserve its integrity (i.e., that the information is not altered). Tools, Data, and Methods used to collect the digital evidence must be designed to reduce or eliminate data tampering to achieve the goal[3]. Stopped digital devices are the primary source of information[4]. Data is not obtained from the primary source by the digital forensics analyst. Instead, the information of that device is duplicated, and the analysis operates on the duplicate. Static acquisitions ensure data integrity by creating a second copy of the device's content (imaging).

In order to check if the replica is an identical complete copy, a cryptographic value is created using mathematical calculations for the originating and the duplicate; if they coincide, the copy's content is a mirror image (or redundant) of the original programming. It is crucial to keep in mind that the acquisition, as mentioned earlier, is primarily applicable to computers. A different method is used when making an image from data stored on cellular telephones and similar devices that cannot be physically separated. Both physical and intellectual methods of data extraction are employed. When evidence needs to be physically extracted, such evidence must be searched and

[3] E4J University Module Series: Cybercrime, Handling of digital evidence, https://www.unodc.org/dohadeclaration/index.html,
[4] Ibid.

collected within a digital device, such as a computer's hard disc. Keyword searches (based on investigator-provided terms) and file carving (search "predicated on the top corner, miler, as well as other identifiers") can be used to perform a physical extraction, as can investigating unallocated space and partitions, which separate hard drive segments). Searching for evidence and obtaining it from its location "inhabits reference to the system files of a desktop operating system, that is used to keep a record of the names and addresses of document based on a storage media such as a hard disc" in logical extraction. Digital devices, file systems, device applications, and operating systems influence logical separation. Extraction from current and discarded files, disk storage, unassigned and underutilized space, and encrypted, compressed, and passcode information is all part of a logical extraction process.

Process of gathering digital evidence, detectives gather preliminary information about the cybercriminals case during the identification step. As with a regular criminal investigation, the goal is to gather as much preliminary information as possible. the following questions are being investigated:

1. Who was involved in the criminal activity?
2. Who understands what is happening?
3. At what moment in time was the cybercrime committed?
4. What areas are the target of cybercrime?
5. What are the other circumstances leading up to cybercrime?

Investigations never commence before even determining what sorts of information are sought. In addition to computers and external hard drives (e.g., fridges and clothes washers), digital evidence is saved on smartphones and tablets, smart TVs, smart cameras, and gaming consoles (to mention a few). Digital evidence is preserved on public and private resources (e.g., social media, webpages, and discussion forums). Online backup solutions are employed by a variety of applications, webpages, and digital equipment. Consequently, numerous providers can store customer data in various places, in its total or parts.

Collection

When it comes to cybercriminals, the crime scene is not just the location of the digital devices employed in the offense and that had been the victim of the offense. There are many different types of digital equipment, networks, or websites involved in a cybercrime scene of the crime. As soon as there is evidence of cybercrime, it is time to protect the crime scene. The first responders identify the crime scene and isolate the users of all electronic devices located at the scene to prevent contamination and preserve volatile evidence. Digital devices should not be used further by their users. In the investigation and search, neither the first responders nor the investigator should ask for help from anybody else. If the investigator is not the initial responder, they explore the crime scene for evidence and make notes about what they find—the investigator. The crime scene must first be documented before any evidence can be collected. Throughout the entire investigation

process, documentation is required. This paperwork must include information on the electronic devices acquired, such as how they operate - on or off, standby - and their physical features, such as the model and year of the item, as well as any markings or damage. Sketches, photographs, and video footage of the crime scene and exhibits are also required to record the location and evidence in addition to text notes and reports. The evidence is gathered by an investigator or a crime scene technician. The collecting methods depend on the type of computing device and the formal and informal sources of electronic content for various digital forensics activities in multimedia, video, and mobile.

Using mobile devices and other Internet-enabled things as evidence is a standard operating procedure for law enforcement authorities. Some principles and steps should have been observed to probe cybercrime to ensure the admissibility of evidence acquired in Court and the tools and other resources required to carry out an investigation included in a standard operating procedure (SOP).

The research should be conducted with an eye on identifying any unique constraints that may arise. A cybercrime investigation could involve dealing with numerous electronic devices, software platforms, and complicated network configurations requiring specialist knowledge, variations in the data collection process, and assistance in identifying connections between devices and systems. For example- cybercrime investigators may have to deal with (e.g., the topology of networks). It is necessary to preserve volatile evidence and shut off digital devices before gathering evidence. The collection techniques will be determined by the condition of functioning of the personal technology encountered. Volatile evidence (e.g., temporary files) is saved before powering down and collecting a computer if one is found. If the device is on, however, all of the Data on it will be lost. The method used to acquire digital evidence will be classified by the characteristics of the digital device used during the inquiry. There should be a collection of digital devices and other related materials (such as memos and notepads that might contain password information or other information concerning online credentials), telephones, faxes, printers, and routers, for example). The investigator's actions should be documented during the gathering of evidence. Each piece of equipment should indeed be labeled, wrapped, and returned to a computer forensics laboratory (together with any associated cables or power cords).

Preservation

Digital evidence preservation protects it from tampering. To preserve the evidence's integrity, it must always be handled with care. First responders, researchers, crime scene personnel, and digital forensics specialists must prove that electronic content was still not manipulated during collection and acquisition. It is feasible, but digital gadgets are required. Proving this requires a chain of evidence. The ownership chain is "how investigators retain the scene of the crime and evidence." Included is who obtained information, what and how it has been obtained, and who claimed ownership of the data. It is

important to include facts such as when and why the evidence was relocated when tracing its provenance along the chain of evidence.

V. ANALYSING AND REPORTING OF DATA

The analysis step of digital forensics involves evaluating and interpreting forensic evidence and conveying the conclusions (reporting phase). The analysis stage collects data from the device and reconstructs events. Information obtained throughout the investigative processes and help evaluate the inquiries in this stage must be communicated to the computer forensics investigator in the laboratory (e.g., IP address). Depending on the evidence at the scene sought, assessments may encompass networking and root storage analysis. It determines what, where, and how a file was generated. In addition, it is assessed if it can connect to external storage (cloud). Computers can evaluate time, possession and ownership, program and document, and data hiding. Time-frame analysis is used to create a chronology of events that led to an event or determine when a user completed an action. Computer files were analyzed for their provenance and ownership.

Using programs and files on a computer, investigators can establish the victim's ability to conduct cybercrime. There is now a way to analyze data Data hiding analysis searches for hidden data. In order to hide their operations and identities, criminals use encryption. Forensic analysts may have used data concealing techniques to protect their identity and conduct. Confidential data can indicate criminal intent. These researches seek to retract (or event reconstruction). An event reconstruction seeks to determine who was responsible for what, when, and where. There are three types of event reconstruction: temporal (deciding where events occurred), interpersonal (attempting to determine who was engaged, what they performed, and associated relationships).

To sum up, event restoration for relevant situations imperfect information and evidence to resolve a case. To avoid bias in the outcomes of these investigations, cybercrime attorneys and digital forensics experts must be aware of these restrictions. The findings are published. The assertions should be clear and precise. This should be accompanied by proof such as chain of possession documentation (e.g., figures and graphs along with tool outputs). These findings should be interpreted in the context of the study topics. Less is more. Forensic scientists and investigative policies vary per country, as does the report's substance. Uncertainty about the result must be stated in the text to avoid misinterpretation.

THE INFORMATION TECHNOLOGY ACT 2000 AND THE EVIDENCE ACT 1872

Under 2000 of the Information Technology Act was revised to include "electronic evidence" under the Evidence Act and also the Indian Penal Code ("IPC") ("IPC"). The IT Act but also its amendment are built mainly on Model Law concerning E-commerce. The electronic record indicates data, recording, or data generated, picture or sound preserved, received, or sent electronically. SECTION 4 OF THE IT ACT Reinforces AND USES Digital RECording

Section 92 of the IT Act amended the Evidence Act to have included "electronic record," allowing digital evidence to be admitted. Historically, Sections 63 and 65 of the Evidence Act dealt with one and specified the admission of electronic evidence. The electronic evidence collected by digital forensics was recognized as a "document," too though, as the printed copies were designated additional evidence, needing verification by a qualified signatory susceptible to cross-examination.

Because of these dominant elements of Section 65B of the Evidence Act, mainly related to the admittance of such electronic data, it is an obvious and explicit legislative purpose not to extend the application of Section 59 and 61 to 65 of the Evidence Act to electronic evidence[5].

ISSUANCE OF DIGITAL RECORDS

Section 65A of the Evidence Act permits the substance of digital files to be proved in conformity with Section 65B. Thus, any digital evidence must be demonstrated in conformity and Section 65B of the Evidence Act. A document is termed an electronic recording if it comprises material from documents or interactions written on paper or saved, recorded, or duplicated electronically or physically media created by a computer.

Internet evidence is evidence pursuant Section 65B of the Evidence Act. A duplicated copy (along with a printout) of a genuine electronic copy may be employed under specific technological conditions. These:

a) The computer that produced the electronic version must have been routinely utilized.

b)must have formed in the digital format must have been routinely input into the compacter.

c) The computer-operated correctly;

d) The computer-operated should be an identical version of the original.

As may be observed, the conditions listed above apply to data validity. The criteria ensure that information has not been exploited and that the technology is operating correctly, ensuring the correctness and validity of the duplicated data.

Section 65B(3) of the Evidence Act provides that even if the person uses a system state to store or process the data, all interconnected devices are treated as a single device.

VI. AN ANALYSIS TO SEC 65-B OF THE INDIAN EVIDENCE ACT, 1872

Section 65-B of the Indian Evidence Act, 1872 deals with electronic documents as evidence. The original evidence computer does not have to be presented in Court. The Court may accept a printout or a copy on CDROM, hard disc, floppy, etc. However, specific criteria must be fulfilled, and a certificate is issued. Cybercrime presents a new challenge to law enforcement. Criminal acts are done, and evidence is stored electronically. Also, cybercrime is a reality. These crimes almost usually have digital evidence. Computer security

[5] Ajay Bhargava , Aseem Chaturvedi , Karan Gupta and Shivank Diddi, India: Use Of Electronic Evidence In Judicial Proceedings, Mondaq, https://www.mondaq.com/india/trials-appeals-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings.

specialists should be aware of legal requirements and the growing discipline of computer forensics. The information era is affecting the legal system. The capture, authentication, appraisal, and regulatory admissibility of data stored on ferromagnetic and other media is one key area where this is felt. This Data is known as digital evidence. Digital forensics is the problem with the law of digital evidence. It combines science and law. In the paper realm, the law assumes a procedure that all parties understand and follow. Acquisition, identification, evaluation, and admission are four steps that occur almost automatically. When we apply this technique to forensic data, we run into new issues. Digital evidence is by definition invisible. So other tools besides the human sight must be used to gather evidence. It is only natural that the digital evidence process mirrors the paper evidence method. Using tools or knowledge is required for each step. Hence the procedure must always be documented. The Court must grasp the procedure.

Evidence collection is a complex legal issue. In truth, they are inextricably linked. The legislation states what can be confiscated, when, who, and where. Examining digital evidence determines its nature.

1. Is it a file, a word processor document, or a programme?

2. Examining a piece of evidence may reveal its actual location. Is the document on a computer hard disk or a server in another country?

3. In brief, a technological basis may be required to gain legal authority to search. Similarly, it may need technological abilities to re-search.

4. This phase frequently produces meaningless raw media. Identifying digital evidence is a three-step process. Its physical shape must be defined. That is, it is on a particular medium. Its logical position must also be identified. Where is it in the file system?

5. Finally, we must put the information in the proper context to understand it.

It may be necessary to examine the evidence in machine language (ASCII or EBCDIC) or via an application (program). Each of these processes involves technical expertise and may necessitate trial testimony. We have now converted media into data. Data evaluation requires technical and legal decisions.

Information is data placed in its proper context. Technically, it may even be possible to deduce how, when, and who produced the data. The legal issues are relevance, serviceability, and who can testify.

AUTHENTICITY

Enclosure/Certificate

The non-technical conditions are set out in section 65B(4) of the Evidence Act. The certificate is required to meet the criteria of Section 65B (2) of the Evidence Act. The certificate must be verified by the person responsible for the equipment that produced the data. The certificate should describe the electronic copy holding the assertion, describe its creation, and identify any devices used to prove that a computer has created it. The certification also must address any of the requirements for

admission. The certificate also ensures the source's integrity and authenticity, enabling the Court to rely on it. This is essential because digital information is more easily manipulated.

Prerequisite For Certificate

Is a subsequent validated Segment necessary per section 65B of the Evidence Act?

The Supreme Court reacted in Anwar PV v. PK Basheer and Others. But the goal was something else. Navjot Sandhu v Afzal Guru [(2005) 11 SCC 600] found that compliance with Section 65B of the Evidence Act—which deals with electronic data admission—does not exclude the introduction of secondary substantiation under other parts of the Act, i.e., no certificate, including those of the listing in Section 65B sub-section (4), implies secondary evidence. So the Supreme Court said the legislature could not construe Section 65B. Despite the IT Act of 2000 and amendments to evidence law, it was decided that digital material could only be presented under Section 65B of the Evidence Act. SUPREME COURT ACKNOWLEDGES PROOF ACT PART II, SECTION 65B

The Supreme Court ruled in Navjot Sandhu that evidence must be cleared under Section 65B of the Evidence Act. The Supreme Court says Evidence Act Section 65B replaces Sections 63 and 65. Evidence Act Section 65B covers electronic evidence. Section 65B of the Evidence Act deals with electronic record-specific evidence regulations. The generalia principle suggests that sections 63 and 65 of the Evidence Act should be repealed.

The Evidence Act's Section 65B necessity to observe an electronic record without the equipment is reduced. The Supreme Court says this condition can be eased if it promotes justice. The Supreme Court concluded that just primary processing is required when someone in control of the equipment produces digital evidence. The Supreme Court remanded the matter to a lower court for clarification.

Statement of Accounts

The Banker's Book Evidence Act of 1891 governs this. According to Section 2(8)(c), a bank account book entry should be accurate that include the certification based on Section 2A. The Reserve Bank of India has advised all States and National Co-operative Banks to provide documented evidence and digital replicas to courts as required by law. Without a certificate, a computer-generated book entry would not have been a certified duplicate as specified in Section 2(8), and hence would not be deemed the original entry based on Section 4 of the Banker's Book Act. Submission of declared accounting statements is subject to verification and competence objections[6].

Equivalent reports can be supported by a written or electronic statement with the certification required by Section 65B of the Evidence Act. The fact that the requisite certificate accompanies the duplicate does not nullify it. The designated representative's certificate per Section 65B of the Evidence Act confirms the bank's account statement for national financial institutions[7].

[6] Ibid.

[7] Ibid.

Investigations and Proof of Conduct

The Evidence Act sets certain presumptions for electronic records. If any electronic record claims to be an accord (including electronic signatures from parties), the Court must infer that it is one since it was signed electronically, according to Evidence Clause 85A. Section 85B of the Evidence Act similarly presumes that a secure electronic record has not been altered since it was secured unless proven differently. The Evidence Act supposes the validity of digital Gazettes under Section 81A but assumes the accuracy of an electronic signature certification under Section 85C.

Other Judicial Proceedings in the Use of Electronic Media

Aside from digital records being used as evidence, courts increasingly rely on digital media for additional purposes. To serve a rebuttal party in advertising action or civil lawsuits where interim relief is sought, the Honorable Supreme Court has allowed parties to serve the rebuttal party through email, in addition to the traditional means of service. That the Bombay High Court shared the same opinion. The Delhi High Court and the Bombay High Court have recently approved service by WhatsApp[8].

CYBERCRIME SCENE ANALYSIS IS A DIGITAL STUDY, EXAMINES DIGITAL CONDITIONS AND EVENTS.

When searching for a file on a computer, all computer users go through the basic digital investigative procedure. They were attempting to answer the query: What is the file's complete location named crucial document? Generally, digital investigations may aim to answer questions. A digital forensic examination is a unique situation of a digital investigation where the processes and methods permitted the results to be submitted into a criminal court. The method to ascertain how anyone else accessed a system and identify how much exposure to it is significantly more complicated than authentication and personalization. It is a method of finding evidence and then examining it.

Investigation procedure There is also no single technique for investigating the matter. An intuitive technique is to use the same primary stages performed by authorities at a physical scene of the crime, where we have had a digital scene.

1. The first phase is restoration, wherein we seek to preserve the crime scene so that the information is also not lost.
2. The second point is to search for obvious evidence. The evidence is typical of such investigations.
3. After apparent evidence is found, more thorough search results are conducted to fill in the gaps.
4. Every piece of evidence found may raise questions about its origin.

Cybercrime Probe Inquiry of forensic data and cyber paths found on computer hard drives, cell phones, CD/DVD/floppy drives, computer networks, or the internet. Photos, encrypted files, password-protected files, deleted data,

[8] Ibid.

formulated hard drives, and chat transcripts may also contain these. Basic cybercrime investigation rules. The study results of a cybercrime investigation are only admissible in Court if they follow three basic rules:

1. Cybercrime researchers must be qualified and knowledgeable. This is necessary to conduct the investigation properly, gather material information, and assure the Court of the evidence's admissibility.

2. No tampering or altering of the original digital evidence. The image/clone of the current findings must be used for practical purposes. Otherwise, extra care and prudence must be exercised when working with them based on actual events.

3. An detailed audit trail is required. Audit trail forms and implementation of control forms must be maintained properly. Any discrepancy in these records refutes the investigation's findings.

E-evidence: gathering and extraction First, digital data must be acquired before it can be considered evidence. Collecting evidence at the scene for an investigation or court proceedings is difficult enough without adding digital information to the mix. Computer transactions are quick, anonymous, and do not require handwriting or signatures to identify the parties involved. Computer records are amended, deleted, or only exist temporarily. Worse, some auditing software may automatically delete records after they are finished.

Law enforcement presently uses a computer to catch criminals kudos to the emerging technology evidence forensic evidence. To be used in Court, digital evidence must be stored or transmitted as binary. Those places this can be found are a computer's complex motivation and a phone. Children's pornography and credit card fraud are examples of e-crime. In addition to e-crime, electronic content is being used in other cases. For example, suspects' email or phone files may contain vital evidence about their intent, current location at the time of the incident, and relationships with other suspects. An unsolved BTK mass murderer who had killed at least ten people in 1974 was finally apprehended in 2005. Police agencies integrate computer forensics into their infrastructure to combat e-crime and collect digital information for all crimes. Law enforcement agencies must constantly train officers to gather digital information and keep up with rapid changes in technology such as operating systems.

VII. DIGITAL EVIDENCE ANALYSIS

Assuring the security of data includes assessing the digital forensic processes and instruments used to get it, as well as the expertise and qualifications of the professionals who gathered, stored, and processed it. This examination tries to establish if digital evidence was handled and examined following scientific principles and standards

The digital forensics process; why a specific digital evidence tool was used and not others; how digital evidence was preserved, obtained, and analyzed and interpreted; the perception and conclusions of the analysis conducted, and the accurateness of these understandings; and any alterations that may have occurred to the data.

The digital forensics laboratory's standards and processes are also evaluated for reliability in handling and interpreting digital evidence. The test looks for "reliable techniques, adequate systems and technology, skilled individuals, and reasonable results".

You Should be Aware of these Facts

- Take Action to Preserve Your Safety

Cyber breaches and online offenses can be prevented by taking the appropriate security steps and remaining vigilant when connected. Educate yourself on the best practices for keeping your computer, networking, and private details safe.

- Learn about the most common online crimes and threats.

Business e-mail compromise (BEC) frauds take advantage of the fact that so many of us conduct business via e-mail, both personally and professionally, and it's one of the most financially destructive crimes committed online.

- Stolen personal information like a Social Security number is used to perpetrate theft or fraud in the name of identity theft. This sort of malicious software, known as ransomware, blocks your access to your computer data and systems and demands that you pay a ransom in order to get them back.

- Scammers use spoofing and phishing to fool you into giving them critical information.

- Predators lurking online pose an increasing threat to children and teenagers.

VIII. CONCLUSION

The IT Act and subsequent Evidence Act Amendments have significantly increased the use of electronic records in Court. Despite numerous court rulings requiring certification, it has become a mere formality. It will be fascinating to see how the Supreme Court interprets the certificate requirements under Section 65B of the Evidence Act. The Court should evolve fast in cyberspace to enhance confidence in using electronic records while bearing all practical problems. The spread of digital technology has created a tumultuous social situation. The future of digital forensics has brought with it the issue of admissibility of evidence.

The spread of information technologies has resulted from a tumultuous social situation. It has become quite important in our lives. The never-ending desire for improved technology has bred many vices in society. With the advent of modern technology, criminal activity has taken on a new dimension. We cannot deny the role of intriguing technology in our personal and professional lives. On the scale, we struggle to balance both situations.

The phrase 'cyber' connotes the internet, technology, and virtual environment. For a lawyer or technician, it also means other things. Included in this list are computers and related devices. In a nutshell, they are anything and everything related to technology or the generic phrase 'computer' and its offspring. All of this is referred to as 'cyber space.'

The crooks use high-tech tools to commit crimes that are beyond the comprehension of the average person. Low-skilled in this discipline cannot imagine tracing the crime's roots. It gave us a new term called cybercrime. It is a crime where a computer (or cyber) is either a tool or a target.

In a technological crime, the evidence will likewise be electronic. In the absence of an expert, it is sometimes impossible to verify such evidence. Here comes cyber forensics. In forensics, science and technology are used to understand the basic concepts in Court. The word cyber implies a connection to cyberspace. We call them 'electronic evidence.' They are the collection, preservation, analysis, and presenting of computer evidence in the trial.

*****