ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

THE EVIDENTIARY VALUE OF MODERN ELECTRONIC DEVICES AND THEIR APPLICATION IN THE JUSTICE SYSTEM OF PAKISTAN

Ishfaq Ahmad
PhD Scholar, Lecturer in Law
Bahauddin Zakariya University, Multan Sub Campus Vihari, Pakistan
ishfaq.ahmad_vcamp@bzu.edu.pk
Muhammad Faisal
Lecturer in Law
School of Law, University of Okara
Muhammad.faisal@uo.edu.pk
Muhammad Umair Razzaq
Lecturer Department of Law
The Islamia University Bahawalpur
umair.razzaq@iub.edu.pk
Muhammad Ahsan Iqbal Hashmi (Corresponding Author)
Assistant Professor of Law
Bahauddin Zakariya University, Multan Sub Campus Vihari, Pakistan
ahsanhashmi@bzu.edu.pk

Abstract: Social interaction is facilitated by mental processes shifting from the real world to the virtual world. Computers, mobile phones, printers, digital cameras, and other information and communication technology equipment are crucial to the virtual world. Unlike the physical world, the virtual world provides several opportunities for crimes such as phishing, identity theft, child pornography, hacking, and so on. Electronic data is frequently relevant in demonstrating or disproving a truth or fact in question, the data that is used as evidence in court. In several established judiciary cultures around the world, employing modern Devices for evidential representation is permitted. Modern technology is also being used in Pakistan's courts and judicial system to present evidence in court, which aids in the formation of more informed decisions.The Qanun-e-Shahadat order1984, including its paragraphs and Articles, as well as the Electronic Certification Accreditation Council, established under Section 18 of the Electronic Transaction Ordinance in 2002, clarified the use of contemporary technology to present evidence in courts with the viewpoints of the state and religion.

Key Words: Electronic Transaction Ordinance, Electronic Evidence, Cyber Crime, Modern Technology, Digital Evidence, Electronic Paper, Dying Declaration

Introduction

The current generation is the first to grow up in a digital environment. Electronic writings have developed as a crucial foundation of modern society's communication due to the meteoric rise of electronic correspondence. There are three main factors that have contributed to the development of a paperless environment: the dematerialization of the workplace, the ubiquity, and adaptability

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

of electronic devices[i]. Modern individuals who have access to the Internet are nearly unanimous in their daily reliance on electronic means of communication.

Legal norms based on a more tangible past reality are being tested by the introduction of electronic evidence. Perhaps the greatest difficulty judges face when deciding whether to admit such evidence is establishing its authenticity. While scientific evidence is generally accepted by Pakistani courts (as described above), the courts may reduce the value of such evidence if they believe that it has been tampered with. The courts must also be cautious about accepting fake audio or photoshopped images as evidence.

Electronic Evidence in Pakistan

The legal system in Pakistan has traditionally accepted and made use of scientific evidence and cutting-edge methods. Step one in collecting evidence is locating the scene of the crime. Cybercrime crime scenes can be hard to pin down because of the international nature of cyberspace. Electronically Stored Information (ESI) can be challenging to find and gather since there are so many different types of digital storage devices. By following a thorough procedure, conducting a thorough investigation, and conducting a thorough inspection, investigators from LEAs will be able to locate all relevant ESI in advance of collecting and preserving digital evidence. According to Casey, the first stage in acquiring evidence is to identify potential sources of evidence. Identified evidence frequently contains insufficient or excessive information. If too much information is gathered, search and seizure restrictions may be violated, and if too little information is gathered, exculpatory or incriminating evidence may be overlooked.

Because digital evidence is fragile and easily manipulated, changed, edited, encrypted, and deleted, the investigator's work of identifying the relevant evidence becomes more difficult. Furthermore, "digital evidence is made up of three primary components: binary data, a storage device on which to store that binary data, and software to read and analyze that binary data. Criminals may alter, manipulate, or modify digital evidence in order to erase any traces of its existence from computers, mobile phones, and other computing devices, making it harder for the investigator to track down evidence of such change that may not always be possible to identify. [ii] To modify digital information, criminals employ advanced ways. As a result, digital evidence may be manipulated without leaving any evident indication of a breach, is a well-known truth. As a result, identifying evidence modification involves knowledge and significant effort on the part of LEAs.

When a crime is committed in cyberspace, the investigator's most crucial task is to preserve data retrieved from the crime scene or the equipment used to perform the crime. Because the criminal may erase evidence in many circumstances, the investigator must understand how to recover the data that has been lost or deleted. If the investigator is unable to recover the lost or deleted data or files, the inquiry may be abandoned. In fact, the investigator goes to great lengths to retrieve erased data or files as much as feasible. With the constant growth of technology, it is difficult for LEAs and computer professionals to stay one step ahead of technologically skilled criminals.[iii]

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

Gathering and preserving evidence is the most critical aspect of any criminal investigation. Every type of evidence is difficult to gather at the best of times," but when that evidence is in electronic form, an investigator confronts additional challenges because it lacks the permanency of traditional evidence. To put it another way, electronic evidence collecting is very expensive to collect, the processes are tight and extensive, the systems involved may be unavailable for regular usage for an extended length of time, and data analysis must be completed." In many circumstances, the victim is unaware of the fraud, and the LEA is often notified too late, posing several challenges for the investigator to adequately probe the case and collect appropriate evidence to prosecute the lawbreakers. Evidence can either be useful information for resolving a disagreement or entirely useless information depending on its credibility.

Importance of Digital Evidence:

The most crucial part of a crime and inquiry is electronic evidence. Arresting a criminal without electronic evidence is quite difficult nowadays. There are numerous examples to back up this claim. The following example illustrates the importance of electronic evidence. Because there was no data in modern technologies to confirm or deny the facts, law enforcement organizations were unable to solve the criminal case.

Pakistan's highest courts also recognize the implacability of scientific evidence, which is reflected in the rulings and procedures. instances were found to use the words on the registered legalized website of updating resolved cases in Pakistan from all types of courts "Cases are resolved using "modern gadgets" and "modern proof." The legal system recognizes that some matters cannot be resolved without sufficient evidence and expert aid. Globally recognized devices are likewise permitted to be used as modern evidence in Pakistan under Article 59 of the Qanun-e-Shahadat ruling of 1984.[iv] By implication, In the case repeated the declaration that the Holy Quran and Sunnah did not prohibit the use of scientific and analytical procedures to seek the truth. [v] Instead, the Holy Quran encourages people to seek out and investigate the truth. In instances relating to the offence of the Zina (forcing of Hadood) ordinance 1979, courts require the receipt of sophisticated evidence, which includes DNA testing.

Because of advanced technologies and cybercrime, the Pakistani judiciary is concerned about tampering with such evidence and equipment. Because of Photoshop techniques, it is necessary to be aware of the evidence's mimicry while accepting auditory or visual proof. In a case, it was decided to cross-examine the submitted electronic evidence once it was presented to the court in order to authenticate its legitimacy rather than accept as it is. Pakistani courts are currently modern devices that are Admissible as Evidence with a big issue regarding swift justice satisfying the needs of all.

The current sociopolitical and economic environment has been deemed. This article discusses how electronic devices are useful for the collection of evidence in the 21st century. After the revisions, in accordance with the Qanun-e-Shahadat order of 1984 and Sec.18 of the Electronic Certification Accreditation Council, the research concluded that technological progress was used to portray evidence. Evidence from current technical advances has helped to resolve several

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

cases without current equipment, modes that could be tough to resolve However, some legislation must be improved to establish the significance of modern technologies as evidence in the fight against cybercrime Members of Congress, attorneys, and others Using current procedures, The judicial and forensics communities require specially educated individuals to evaluate the veracity and reliability of evidence. To avoid misuse and abuse, evidence should be handled and destroyed carefully after it has been used to conclude the case. Anywhere else, there is wrongdoing. Furthermore, everyone must be confident in the accessibility and validity of current gadgets. Pakistan's crime rate must be reduced by all social groups.

Orientation of Electronic Evidence

General Introduction:

The movement of thinking from the physical to the technological environment is how societal communication takes place. Computers, mobile phones, printers, digital cameras, and other information and communication technology equipment are crucial to the virtual world. Unlike the physical world, the virtual world provides several opportunities for crimes such as phishing, identity theft, child pornography, hacking, and so on. Electronic data is frequently relevant in demonstrating or disproving a truth or fact in question, the data that is used as evidence in court.

This article contends that, while the ETO 2002 declaration is exemplary in that it clarifies the situation with computerized proof while simultaneously reducing the courts' absolute reliance on article 164 QSO, which is in general a lenient rather than mandatory arrangement that fails to impress anyone in its wording of making sense of what is an advanced gadget. Nonetheless, based on a few judges' perceptions of Pakistan's matchless courts, it appears that the proof has been declared necessary and equipped for qualifying the best proof test to the degree of its acceptability, but its value or weight is still passed on to the court's tact. As a result, it may not be incorrect to suggest that advanced proof is still corroboratory proof in terms of weight. There is a contrast between PC put away and PC manufactured proof when it comes to vital proof. Because ETO 2002 only recognizes vital proof that is unique and unaffected despite regular increases or decay, the PC-created proof appears to qualify for example, in the testing of the invention, swap receipts because no further duplicates can be made after the first. The PC put-away proof, on the other hand, should be regarded with a grain of salt because it is frequently altered or added to. As a result, it is frequently treated as corroboratory. The paper will argue that to value rather than dismiss electronic proof, it should be weighed against dependable factors such as genuineness, constant quality, a chain of authority, and dependability, as outlined in internationally regulated methods.

Modern-day Reliance on Digital Evidence:

The need to rely on digital evidence has grown exponentially as information technology has advanced. Digitally created or electronic documents are utilized in place of paper. For example, professional and informal letters, applications, and even invites have all been supplanted by emails. Similarly, vocal talks over the phone have been replaced with immediate text messaging.

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

Images taken using a digital camera are utilized instead of photographs taken with a camera in the past. [vi]In light of these conditions, it became necessary to adapt our evidence laws to meet the demands of digital evidence. Simply said, our lives have become so reliant on technology that everyone living a normal life while being connected to the so-called world must be using some type of technology.As a result, everyone is leaving digital traces of their interactions with technology. Because many acts in modern society include the use of technology, criminals are using it as well, creating trails for digital forensics to follow in order to reveal their crimes. For example, someone who engages in harassment, child pornography, or even kidnapping for ransom is likely to leave digital evidence of their actions. However, proving these crimes was difficult in the past since our courts relied on traditional techniques of gathering and presenting evidence, which worked fine when dealing with oral or documentary evidence but required significant adjustments inadmissibility.

Consequences of Electronic Transactions Ordinance (ETO) 2002

This concern was eliminated with the passage of the Electronic Transactions Ordinance (ETO) in 2002. The changes it has brought about plainly indicate that information extracted digitally, whether in the form of a document, transaction, conversation, or audio-visual image exchange, cannot be disregarded solely because it is in digital form. Such evidence is not only significant, but it is also admissible if it is direct rather than hearsay.

Digital evidence was only allowed under one provision of the QSO 1984, namely article 164, before the enactment of ETO 2002. According to it, the court has the authority to enable any evidence obtained by modern means to be produced and acknowledged if it deems it acceptable.

Article 5 of ETO Ordinance 2002

Another alteration in the admissibility of digital evidence was brought about by Article 5 of the ETO. If digital evidence is full and pristine, it will be admissible evidence regardless of additions made organically or by accident, according to this article.

Article 46 and Article 73 of QSO

Similarly, digital evidence or evidence derived or kept through mechanical processes is applicable, according to Art 46- A of the QSO. This page supplements QSO's article, which states that evidence may only be given in relation to issues or pertinent facts. Similarly, an explanation to Article 73 QSO has been added, stating that all electronic papers, including electronic documents, are primary evidence.

Digital Evidence in the Twenty-First Century:

In recent years, the usage of digital gadgets has increased exponentially in all types of activity. All correspondence, for example, is done via email or instant messages. Similarly, digital photos have supplanted traditional photography. The contract's provisions are spelled out in digital

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

papers, and the contract is likewise accepted digitally. However, there is a significant distinction between digital and everyday activity. All of the steps in a digital action may be traced; in other words, digital activity leaves a traceable record. For example, recovery of the data is possible from computer files even if it was removed or deleted. While deleting something leaves room on the storage device, whether it's a hard disc, USB drive, or floppy disc, it can be detected via online storage engines like cloud or through the network administrator. In other words, any action taken on a digital gadget can be tracked. When something is done physically, on the other hand, it is possible to erase all evidence of your wrongdoing. As a result, digital evidence has become increasingly important since the turn of the century**.** This gets us to the point where digital evidence must be defined.

According to Section 27 (b) of the Anti-Terrorism Act of 1997

A person may be convicted based on electronic or forensic evidence, whichever is obtained by current means.[vii] Nonetheless, Pakistani legislation is silent on how electronic documents would be authenticated. The methods of authentication described in the Qanun-e-Shahadat Order and the Electronic Transaction Ordinance are relatively broad and thus ambiguous.

Only writing that electronic documents are acceptable, and convictions are based on electronic evidence is not enough in this day and age of current technology. It is an era in which the law elaborates the procedure to reduce uncertainty among lawyers, judges, and the general public. The judiciary can play an essential role in developing these regulations in this case. However, the majority of the cases detail the types of evidence that can be used in court. For example, in the case of Salman Ahmad Khan v. Judge Family Court, the Multan case court allowed the applicant to record her statement through a video link.

Article 164 of the QSO 1984 allows for the recording of evidence using modern equipment, according to the court. In another case, Asfandyar v. Kamran, the court held that CCTV material can be used as a preview of article 164. However, "the mere provision of the use of Video as proof in a legal proceeding was insufficient to rely on it unless it could be established that it was authentic"[viii] It was the responsibility of the defense or prosecution to interrogate the individual who prepared such material from the CCTV system to verify its authenticity. The burden of proof rests with the defence or prosecution to question the person responsible for preparing the CCTV footage.

In another case, the court stated: Information transmitted through advanced technology like SMS —Such information was validly accepted, Despite the availability of global methods of communication, it was constantly crucial to have a testimony there when such material was transmitted or collected in order to verify the reality. -Although modern gadgets were legally permissible under Art 73 of the QSO, 1984, the proper procedure had to be performed to prove a truth.

Electronic evidence is now an integral aspect of procedural laws as well. Unfortunately, Pakistan's civil and criminal procedural laws are completely silent on current technologies and

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

procedures, such as electronic discovery and electronic search and seizure. This faulty justice system causes significant delays in resolving complaints.

As a result, the evidence of new technologies is also considered in the family court after the verification and investigation procedures. In another case, The High Court also ruled on ignoring traffic signs and laws and driving recklessly, Modern technology provided proof of this.

This rule is followed by both Islamic and English law. Whatever the best evidence is, it must be pursued in a court of law. In courts of law, first-hand, original, and primary evidence is reliable for adjudication of disputes between litigants. This guideline is typically followed when it comes to documentary evidence, but it is less relevant when it comes to electronic evidence. The photocopies are identical to the primary evidence because the evidence is generated by an electronic system. These photocopies are treated as primary evidence in this case. The Pakistani legal system takes the same method. Pakistani law's original writing rule was based on the rules of other western countries.The original writing requirement is addressed in Section 4 of the ETO, which was enacted in 2002.

As courts struggle with this new technological frontier, it's critical to remember that electronic evidence is subject to the same evidentiary rules as paper documents. However, the unique character of e-evidence, as well as the simplicity with which it can be manipulated or fabricated, raises admissibility challenges that other types of evidence do not confront. The court relied on both oral and documentary evidence. Because everyone feels or observes with their senses, oral evidence is frequently full of inconsistencies and human mistakes. Even documentary proof can contain inaccuracies. Electronic evidence calls into question previous evidentiary norms based on a more concrete world. The most challenging difficulty in determining the admissibility of such evidence is its authentication.

Judges are frequently asked to rule on the admissibility of electronic evidence during trials. The outcome of civil litigation or the difference between a defendant's conviction and acquittal could be determined by how the court rules on admissibility issues. This technological equipment can be used for both legal and illegal purposes. When information recorded or kept in a computer's memory is printed out on paper, it is difficult to say if the version in the memory is a document. It's also difficult to say whether the printout is an original or a copy. Even if such things as audio, tape recording, videotape recording, electronic mail on a computer screen, and electronically sent directives in commercial transactions can be treated as documents when offered as proof. The widespread use of computers, the social impact of information technology, and the ability to store data in digital form have all necessitated changes to Indian law to include rules for the evaluation of digital evidence.

IN PAKISTANI COURTS, THESE ELECTRONIC DEVICES ARE USED AS EVIDENCE:

As previously stated, the Pakistani judicial system generally accepts scientific evidence; nevertheless, because modern procedures and equipment are prone to tampering, the court may

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

reduce their evidentiary value if it believes that such instrument and technique has been tempered.Courts must also be aware of mimicry when accepting audio and the use of Photoshop techniques when admitting photos into evidence.

In Pakistan, scientific evidence and sophisticated methodologies have been accepted and applied in the legal system. There was no reference to modern and scientific technology/evidence to examine the truth and reach a suitable conclusion of the trial prior to the implementation of Qanun-e-Shahadat in 1984. As a result, Article 164 was added to the Qanun-e-Shahadat in 1984, along with the following mention: "Production of evidence made possible by modern equipment or techniques: in such instances as the Court considers appropriate, the Court may permit the production of any evidence made possible by modern devices or techniques." The wording of "modern technology or procedures" is a major focus of this newly implemented regulation.

Following the implementation of Article 164 and the insertion of Article 2(e) in the definition clause of Qanun-e-Shahadat in the year 2002, there has been a significant change in the discovery of modern evidence in our legal system, with decisive results. The trial's duration has been decreased, and expert opinions have taken precedence over the adjective legislation in easing the regulations. Evidence obtained by modern equipment such as cell phone data, tape recorders, video film, video cassettes, fax, email reporting, Polygraphic testing, trace bullets, and DNA tests has been made usable in our legal system. Even the courts have authorized video recording during investigations, eventually allowing it to be used in court.

DNA Profiling:

Because it is a chemical examiner's report and an output of modern technology, the DNA (DEOXYRIBONUCLEIC ACID) report is admissible as evidence. It is also being assessed in light of Art 59 QSO, 1984. In some circumstances, a DNA report is conclusive proof. The admissibility of a DNA result is twofold: in situations of paternity and in cases of sexual offences. DNA testing for paternity is prohibited under Article 128, QSO, 1984. The DNA test report is regarded as corroborative evidence; however, the court has the authority to request a DNA test to evaluate the veracity of allegations, but only with the cooperation of the parties and not on a routine basis. The legitimacy of DNA test reports has been questioned, primarily due to human error, yet in the recent **Zainab Ansari case**, the trial court only relied on the DNA test findings and sentenced the accused to death.

When modern evidence is received and our law courts rely on it, a reference is obtained from the case law recorded in M. Shahid Sahil V. State,[ix] which is copied below in its whole. The Court of Law finds that some cases requiring expert testimony cannot be decided without the participation of experts. In other words, the experts' view would be treated as a complete judgment of the Court. The rules are eased in other ways, and the experts' testimony is recognized a relevant fact. As a source of modern evidence, we can learn about DNA testing, fingerprint analysis, luminal tests for blood evidence, surveillance film, cell tower data, and polygraphic tests under Article 59.

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

The 1984 Court could accept any evidence accessible because of modern equipment or techniques to be produced under Article 164 of the Qanun-e-Shahadat. The Holy Quran and Sunnah do not prohibit the use of scientific or analytical methods in the pursuit of truth. The Holy Quran and Sunnah, on the other hand, actively encouraged discovery and investigation. In cases involving the Offence of Zina (Enforcement of Hudood) Ordinance, 1979, courts had full authority to allow evidence to be received, including the use of DNA tests if necessary.

BASIC EVIDENTIARY STATUS OF ELECTRONIC EVIDENCE:

It's about admissibility and the correct has to be proved afterward. In Art 46 of QSO,1984 the Dying declaration, if the statement of the dying person is being recorded in audio form by the magistrate, then he has to come to court and be a witness there is no further need for corroboration. If the police have recorded those statements in audio, then the presence of two witnesses is necessary. Evidence is a statement or document that can be used in court to make a decision, and scientific evidence is evidence that is created or obtained using computers or modern equipment.

To be accepted in court, digital evidence must be admissible, precise, authenticated, and accurate. Because digital evidence is inherently delicate, it must be handled with care. A detailed digital forensic technique aids forensic investigators in acquiring evidence that can be used in court. It is firmly established that only relevant, material, and competent evidence is allowed in court and that its probative value outweighs any detrimental effect. Digital evidence is not unique in terms of relevance and admissibility, but since it can be easily replicated and edited, frequently without leaving any traces, it might pose unique competency challenges. To maintain the admissibility of digital evidence, the International High-tech Crime Conference developed the following rules in 1999:

- Action taken after seizing digital evidence should not modify that evidence.
- When access to original digital evidence is required, that person must be forensically competent.
- Any activity involving the seizure, access, storage, or transfer of digital evidence must be adequately documented, maintained, and accessible for inspection.
- While digital evidence is under their control, an individual is accountable for any activities performed with respect to it.
- These principles must be followed by every agency that is responsible for seizing, accessing, storing, or transferring digital evidence.

Since April 2013, the new Central Monitoring System (CMS) has been operating. The CMS would also make it easier for government authorities to tap phones without permission. As a result, sufficient safeguards must be developed, or the right to privacy provided by Article 21 of the Constitution will be jeopardized. The resolution of the question is made more difficult since tape recordings can be tampered with by transposing, removing, or inserting words or phrases, and such adjustments can go undetected and even avoid technical specialists scrutiny.

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022

Conclusion

In conclusion, while there is no debate about the relevance and admissibility of digital evidence, it does require confirmation by independent evidence in the majority of cases. Different types of digital evidence necessitate different levels of technical knowledge as well as different levels of caution when relying on digital evidence, and reliance on digital evidence can only be made when its authenticity has been proven to the satisfaction of both the expert and the court.The passage of legislation may not be sufficient to address issues originating from technological advancements that have given rise to electronic and computer evidence. It is also necessary to develop the necessary skills among investigators, computer forensic experts, lawyers, and judges in order to deal with issues arising from such evidence, as well as to provide the necessary equipment and infrastructure for the Courts to deal with the challenges posed by this new field of evidence.

To speed up the judicial process and increase transparency in the legal system, the entire judicial system requires urgent modernization and upgrade through E-governance in Judiciary. The Indian evidence law has progressed as a result of its ability to withstand the stresses and challenges of technology and the cyber world. Our judiciary has adopted suitable revisions to Evidence Law, demonstrating pro-activity. In order to successfully overcome obstructions in trial procedures, law enforcement agencies and investigative officers, in my opinion, must update themselves on the authentication method stipulated by the court regarding the admissibility of electronic/digital evidence. The fundamental necessity of recent times is proper training of law enforcement agencies in handling cyber-related evidence and the application of procedures and sections of Evidence Law when presenting such evidence in court. However, considerable work remains to be done to make it fully capable of dealing with any technology-related difficulties.

References:

Gokul Sundar K. Ravi, “RELEVANCY OF ELECTRONIC RECORDS AND ITSADMISSIBIL ITY IN CRIMINAL PROCEEDINGS” <https://www.coursehero.com/file/80968653/Relevancy-of-Electronic-Records-and-itspdf/> accessed December 13, 2022.

Muhammad Saleem, “Qanun-e-Shahadat Order” (*Qanun-e-Shahadat Order | Muhammad Salee m - Academia.edu*) <https://www.academia.edu/7493194/The_Qanun_e_Shahadat_Order> acces sed December 13, 2022.

Thomas A. Johnson Taylor & F, *Forensic Computer Crime Investigation* (1st Edition, CRC Pres s 2013) <https://www.taylorfrancis.com/books/mono/10.1201/9781420028379/forensic-compute r-crime-investigation-thomas-johnson>.

Richard Boddington, *Practical Digital Forensics by Richard Boddington - Ebook | Scribd* (Packt Publishing 2016) <https://www.scribd.com/book/365187900/Practical-Digital-Forensics>.

John R Vacca, "Computer Forensics [Electronic Resource] : Computer Crime Scene Investigatio n : Vacca, John R : Free Download, Borrow, and Streaming : Internet Archive" (*Internet Archive*) <https://archive.org/details/computerforensic00john> accessed December 13, 2022.

SANAH ASHRAF, BASIS OF EXPERT TESTIMONY IN COURT OF LAW, "June 2015" (*Ju ne 2015*) <https://www.pljlawsite.com/2015art9.htm> accessed December 17, 2022.

PLD 2010 FSC 215

Shahbaz A Cheema, "DNA Evidence in Pakistani Courts: An Analysis" (*HeinOnline*) <https://ho me.heinonline.org/> accessed December 17, 2022.

Pervez Musharraf through Attorney v. Pakistan PLD 2016 LHR 570

Hameed, Usman, Zarfishan Qaiser, and Khushbakht Qaiser. "Admissibility of Digital Evidence: A perspective of Pakistani Justice System." (2021).

27 (b) Anti-Terrorism Act of 1997

PLD 2017 698 2016 SCMR 2084

Munas Parveen v. ASJ PLD 2015 231

PCRlJ 125 2017

Adegboro, A M, the Relevance of Electronic Evidence in the Nigeria Legal System. Long Essay. Igbinedon University, Okada, Edo State 2008, p45.

2017 PCRLJ 1009

Azeem Khan v. Mujahid Khan 2016 SCMR 274

A case of Sexual Abuse of 7 years old minor girl in District Kasoor.

PLD 2010 FSC 215

Louis Strydom, Computer Evidence, 2nd World Conference on the Investigation of Crime, ICC D urban, Dec. 2001. R. v. Robson [1972] 2 All E.R. 699s

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol. 6 No.2 2022