

**Forensic Evidence under Domestic Law: An Efficient Substitute to ocular account in
Pakistani Courts**

Sehrish Neik Ch

sehrish.law@pu.edu.pk

Assistant Professor, University Law College, University of the Punjab, Lahore, Pakistan

Sumia Azhar

sumia.azhar@giu.edu.pk

Lecturer in Law, Green International University, Lahore, Pakistan

Asma Niazi

asma.niazi@giu.edu.pk

Lecturer in Law, Green International University, Lahore, Pakistan

Corresponding Author: * Sehrish Neik Ch sehrish.law@pu.edu.pk

Received: 09-03-2025	Revised: 10-04-2025	Accepted: 21-04-2025	Published: 24-04-2025
----------------------	---------------------	----------------------	-----------------------

ABSTRACT

With the beginning of digital technology, it has transformed the background of evidence, its data collection and settlement of disputes in legal systems globally. In Pakistan, the forensic evidence has speedily swapped off the oldest method of evidence gathering with reference ocular account which used to be heavily relied upon. This article will observe the implication of digital evidence with reference to the Pakistan's legal system, to spot on the importance of new system as compare to old techniques used to be followed in this region. There is a remarkable transformation in the field of forensic science, due to advancement in equipment and changes in legal tradition practices. This research examines the old precedents, their authenticity and present laws, their compatibility with the current situations during litigations. In the end it also provided the recommendations and suggestions to improve the system of judicature to facilitate the litigants with the new trends.

Keywords: Forensic science, Digital evidence, ocular account, Judicature

INTRODUCTION

Digital evidence (hereinafter DE), defined as non-substantive and perishable evidence, is increasingly important in the modern world due to its diversity, complexity, and accuracy, making it the most fragile type of evidence" (Mukasey, Jeffrey, & David, 2008). The Doha Declaration defined digital evidence as binary information that can be produced before a court and relied upon by the court (UNODC, 2021). Digital evidence, found in various devices like cell phones, CDs, and computer hard disks, is often linked to electronic crimes like child pornography, hacking and fraud (Zahoor, 2022). Digital forensic science involves analyzing, attaining, and utilizing digital proof during inquiry proceedings or criminal trials. Established in 1984, FBI and other Law Enforcement Agencies (hereinafter LEAs), it involves the Computer Analysis and Response Team (hereinafter CART), a professional specialist in the FBI Department, requiring cooperation from other LEAs.

In the 16th century, European medical officers began collecting information on death patterns and causes. Italian surgeons introduced modern pathology, while French physician introduced a treatise on forensic medicine. Germany implemented a police medicine system in the late 17th and early 18th centuries. Swedish chemist "Carl Wit Helm" invented arsenic oxide modus operandi. In 1784, compressed paper was

used to protect powder and ball in weapon muzzles. Forensic science involves the use of scientific or technical methods for identifying, analyzing, collecting, and explaining evidence in legal proceedings, encompassing various disciplines with their respective methods and procedures (Arshad, Aman, & Oludare, 2018). This research proposal investigates the use, admissibility, and impact of forensic and digital evidence in Pakistan's evolving legal system. It aims to evaluate their effectiveness in enhancing the reliability of legal outcomes and replace ocular account.

Over the past two decades, significant shifts in Information Technology have made digital evidence collection and analysis crucial for court cases and crime solving, with law enforcement agencies increasingly relying on digital evidence for victim and suspect information. Digital evidence has four phases: preparation, collection, analysis, and presentation. Preparation involves identifying tools, collection involves acquiring and preserving sources, analysis involves dissection, reconstruction, and documentation, and presentation involves communicating findings to stakeholders (Homem, 2018). In Pakistani courts, evidence is presented on two sets of facts: the "ocular account" and "relevant facts", also known as Circumstantial Evidence.

Forensic Medicine, originally Medical Jurisprudence, regulates medical conduct for registered practitioners. Digital evidence, stored on electronic devices, is collected when seized for examination (NIJ, 2008). Digital evidence is now admissible globally, with varying criteria mechanisms across states. Pakistan is gone through various amendments to its domestic laws especially law of evidence to align with modern trends, including the Qanoon-e-Shahadat Order 1984, Electronic Transaction Ordinance 2002, Prevention of Electronic Crimes Act 2016, Investigation for Fair Trial Act and Rules 2013, Federal Investigation Act 1974, and Anti-Terrorism Act 1997. Articles 46-A, 59, 78-A, 164 of QSO 1984, Sections 164-A, 164-B, 509, 510, 510(A) of CrPc 1898, Section 21-B of ATA 1997, and PFSA, 2007 Section 9 (Zahoor, 2022).

LEGAL FRAMEWORK ON DIGITAL EVIDENCE IN PAKISTAN

Digital evidence, also known as electronic evidence, is crucial in modernizing the justice system and addressing technological advancements. DE is very important in the current world its being accurate and perfect piece of evidence. It is information gathered and communicated in binary form, which can be presented in courts as ocular account or circumstantial evidence. Forensic medicine, also known as Medical Jurisprudence, regulates the code of demeanour for legalized consultant and includes DNA, fingerprints, bite marks, and tool marks. The justice system in Pakistan has become more modernized as compare to previous years because of the implication of new tool and techniques to extort evidence. Across the world, several countries have agreed upon the admissibility of DE.

Admissibility: The QSO 1984 has exclusionary rules that may make a fact relevant but not admissible as evidence. Admissibility in a court depends on relevance, a logic-based issue, and evidence rules, while determine whether a rationally probative matter is integrated or not. Admissibility involves relevance and supplementary criteria set by rules, requiring evidence to pass specific tests and external policies. Its not necessary that all relevant evidence is admissible (Iqbal, 2018). The admissibility of evidence is determined by its probative value, which is its relevance, and its proof, which is determined by the evidence's weight (Karim, 2020). Common law views relevance as a factual question, while admissibility is a legal inquiry. Judges determine collateral facts like witness sanity and expert method during trial (Bartlett v Smith, , 1843).

According to Article 2 of the QSO, 1984, a fact is considered relevant to another only if it aligns with the provisions outlined in Articles 18 to 69 (QSO, 1984). Article 131 of the QSO, 1984, empowers the judge to admit or reject evidence during a trial (QSO, Article 131, 1984). In cases where direct evidence for a fact

in question is unavailable, circumstantial evidence, including forensic and digital evidence, can be presented as substantive evidence. The QSO, 1984 clearly stated that “not all logically relevant facts are legally relevant”, transforming logical relevancy into legal relevancy. This provision is saved under Article 18 to 69, which is helping them to be admissible in evidence (Khan, 1993).

QSO 1984 and English Law: The Q.S.O, 1984 differs from English Law in its principle of relevancy and admissibility, requiring evidence to align with relevant and admissible criteria, while English law generally permits all evidence except for best available evidence (Prabhas C. Sarkar, 1913). John Henry Wigmore's "A Treatise on the Anglo-American System of Evidence" highlights the evolution of the legal system, which has embraced rational methods and introduced new forms of evidence to protect against personal biases and emphasize reasoned conclusions (Wigmore, 1923). Wigmore's perspective emphasizes that actions with harmful consequences should not be pursued, while Sir James Stephen's 1876 Digest of Evidence highlights negative rules in the law of evidence. Evidence production should only be excluded if harm outweighs benefits (State v Benner , 1874).

Modern evidence, including electronic and digital, is now admissible globally. Pakistan has amended its law of evidence to align with modern trends and Information Technology advancements. Key contributions include the ETO 2002, PECA 2016, IFTA 2013, ATA1997 and QSO 1984 was a decree introduced by Gen Zia Ul Haq to incorporate Islamic provisions in 1872 Evidence Act. The purpose was too re-established and strengthens the law of evidence while incorporating Islamic teachings and digital evidence. The order introduced new Articles and amended existing ones, including the incorporation f digital terms (QSO, Article 2 (e), 1984). Making information produced, obtained, or stored by automatic information systems relevant is the goal of the amendment, Article 48(a) (QSO, Article 48, 1984).

"Opinion of expert" article has been changed under QSO while adding the relevant article in such words like "authenticity and integrity of electronic documents made by or through an information system" and making information about the "functioning, specifications, programming, and operation of an information system" pertinent” (QSO, Article 59, 1984). The proof of electronic signatures and electronic documents in QSO, which stipulated that if an electronic document is made or signed using an information system, the security method must be demonstrated if it is denied (QSO, Article 78-A, 1984). In order to facilitate the production of evidence derived from contemporary technology, another article was added. The court may permit the introduction of evidence gathered using modern tools and methods, according to this article. The judge also acknowledged the validity of the legal convictions based on electronically created evidence (QSO, Article 164, 1984).

Evidence admissible in court must be relevant, credible, and not violate legal rules, with electronic records influenced by the hearsay rule and best evidence rule. Hearsay is a legal concept that is generally inadmissible in court proceedings due to the preference for first-hand information. Witness’s testimony can base on experiences while confirming their accuracy and efficient cross-examination. However, exceptions have evolved, to allow definite documents to be acknowledged as evidence. For instance, evidence from computers or electronic devices can be considered authentic or undeviating evidence, as long as there are no defects. The best evidence rules prioritize using original records or documents, with copies given lesser burden. Exceptions exist when lost, impractical, or held by the opposing party. Digital evidence, like log files or database entries, can be challenging to identify. Legislation addresses admissibility of digital evidence, especially when opposing parties dispute the accuracy or integrity of printouts.

The main objective of the Electronic Transaction Ordinance, 2002 (ETO), was to make digital and electronic evidence admissible and to end any denial of its admissibility based only on its digital format (ETO, 2002). The definition provided under ETO regarding digital format is being stated that, the purpose of this law is to identify and assist the documents, their records and information, its process of

communication, and dealings in electronic format and to provide for official approval of documentation service providers. Despite being influenced by UN treaties, the preamble's utmost vital function is to facilitate domestic laws. With comparison to other states, Pakistan sought to look up its law of evidence (QSO, 1984) by implementing such modern laws and adding changes with the need of hour. The ETO is divided into 51 sections spread across six chapters. The ETO is a crucial legislation in Pakistan, recognizing and facilitating the admissibility of digital evidence in court proceedings. It facilitates digital format of evidences across all platforms and encourages the system to mull over digital evidence/forensic science without negating it only on ground of its being digital format.

The ETO also combats the condition of affirmation for digital evidence through strict witnesses or evidence format. The ETO, 2002 is mainly deals with electronical business matters, encircling digital accounts and connections. It has great role to define, recognize and facilitating a detail of digital evidence. Pakistan holds a one of best example to establish standards of proofing E-evidence in all legal platforms. The ETO, 2002 has been a landmark in DE, cyber crimes, forensics, and investigation, redesigning the trend of required corroborative evidence for its acceptability. The rise of electronic communication in business has raised legal challenges, especially regarding electronic signatures in transactions. Many countries even don't follow the proper formats to established the online/digital format of contracts with reference to its online/electornical signature and follow the most simplest formats as ordinary one. Lack of provisions for electronic signatures in their contract laws, making online contracts similar to ordinary ones. UNCITRAL overcome this situation by speaking uo to these issues while setting up the lawful importance value of computer and its database, their records, budding a Model legislation on E-commerce, and probing computer accounts as evidence during litigation. Section 29 of the Prevention of Electronic Crimes Act, 2016 requires investigative agencies to analyze data for admissible evidence. Computer/cell phones can be targeted, used for offenses like identity theft, fraud, and pornography, or used as means to commit crimes like information storage. Digital evidence admissibility guidelines require expert witnesses to possess expertise, be independent, and provide objective, balanced opinions. Principles include a demonstrable, objective procedure, qualified individuals, and adherence to relevant formalities (Khan J. (., 2005). Digital evidence is only allowable if pertinent to the issues, and courts must accept scientific techniques within the scientific community. Standard procedures must be followed for scientific techniques to be admissible in evidence (Gumbley v Cunningham, 1988).

Directive Principles for Digital/Forensic Evience in Diverse Regions

American Law Reports and their legal system developed a protocol for police investigating agencies. Same system has been adopted by UK police. Key proposal needs and include maintaining compact record of evidences, recognizing E-evidence's unique nature, replicating operations, applying traditional evidence rules to digital evidence, and establishing a clear chain of custody and conclusive report to establish authenticity, reliability, and accuracy of evidence. The increasing prevalence of digital devices in the UK has led to a greater demand for digital forensic techniques, exacerbated by the growing volume of data stored on these devices. Law enforcement and intelligence agencies conduct numerous digital forensic analyses, serving various purposes such as providing evidence of criminal activity, exonerating suspects, or aiding investigations. Many commercial channels seeks the help of digital techniques for their departmental level investigation. The Metropolitan law enforcement agency also inspects and has surveillance almost 40,000 devices yearly, examining various resources such as smart phones, Wi-Fi routers, GPS equipment, CCTV, and more through which a digital crime may happened. The Digital Forensics needs and includes how to recover data, its interpretation and later to present it. UK legislature make it more easier while searching and attainment of data on devices legally apprehended, intercepting communications with warrants, and acquiring data through equipment interference (HOP, 2016).

Forensic evidence in the USA is regulated at federal and state levels, with guidelines from NIST and FBI. Digital evidence is increasingly used in court proceedings, addressing issues like electronic discovery, data privacy, and cyber security. Inadmissibility completely depended upon the relevance depends on relevance and chain of custody, with expert opinion. Digital evidence is broader, more sensitive, and mobile, requiring distinct training and tools. The rise of personal electronic devices highlights its importance, with interconnected criminal justice implications. Forensic evidence analysis involves using appropriate techniques to determine the crime scene and solve it. Forensic experts must be knowledgeable about handling and examining forensic evidence, including identification, collection, preservation, transmission, and examination. Courts do not rely only on forensic evidence exclusively but it needs to seek help of experts. Digital evidence, including computer audio, video, recordings, and images, is also considered (Hameed, Zarfishan, & Khushbakht, 2021). Computer forensics involves investigating various types of digital evidence, including hard drives, storage media, cell phones, cameras, GPS devices, thumb drive machines, and gaming devices. Digital evidence can be altered and obliterated, with erased data remaining in an unallocated space. Overwriting software can be used to wipe a drive clean by repeatedly writing data until the disk is full and free of space. Computer data stored in crime scenes may be at risk, so securing and searching for digital evidence, including computers, cell phones, and other devices, is crucial for solving crimes.

Comparative Analysis of Digital Evidence with Urbanized States: In advanced nation states like the United States, United Kingdom, and northern Europe, forensic techniques and technology are more advanced and sophisticated than in Pakistan. They have security cameras and crime scene photography, while the public in Pakistan is often careless and unaware of the value of forensic evidence. In the most of developed states, forensic science has been prioritized as special branch of educational sector in almost all institutions, and the public is already well aware about their duties like how to respond and to inform during any crime vista. Here in Pakistan, crime vistas cannot be taken over due to limited equipment, techniques and training among public. The evidentiary value of forensic evidence in Pakistan is low compared to advanced countries (Goodison, 2015).

Critical Evaluation of Forensic and Digital Evidence with ocular account: The intersection of subjective human perception and objective scientific analysis in legal contexts is crucial for evidence collection and presentation within judicial systems. Ocular account such as testimonies of eyewitness and visual observations is considered trustworthy in criminal matters if corroborative evidence is supportive. In Pakistan, digital evidence has been elevated to primary status due to legislative changes, such as the Electronic Transaction Ordinance 2002 (ETO), which affirmed the authenticity of electronic documents, information, records, and transactions. However, the evaluation and weight of digital evidence remain subject to the discretion of the court, indicating that digital evidence still carries a secondary nature (Wahab, 2024).

CHLLANGES TO DIIGITAL EVIDENCE: Investigators face challenges accessing data due to encryption or cloud storage, and potential use of anti-forensics techniques by criminals. Encryption is crucial for safeguarding sensitive data, but certain forms can impede investigations (Casey, 2011). Encryption is the process of encoding data to only be deciphered by authorized recipients. It is used for data storage, online communications, and transit data. Currently, most devices can activate optional encryption, but manufacturers are increasing default encryption, potentially making digital evidence less accessible to investigators.

- **Cloud Storage:** Cloud computing widespread use presents a significant challenge for digital forensic practitioners due to rapid changes in data storage, potentially leading to data loss and complicating verification efforts. Cloud services are less likely to store users' data locally, making forensic techniques less effective. Law enforcement agencies can request cloud data directly from

providers, using Mutual Legal Assistance Treaties to issue warrants for retrieval, though this process can be slow.

- **Anti-forensics:** Criminals often use anti-forensics techniques to conceal their digital activities, often in complex cases. These practices include altering file dates, permanently erasing files, and using encrypted storage with multiple passwords. These practices can lead to investigators suspecting missing evidence. However, some individuals also use these methods to protect data and privacy. The value of forensic evidence depends on scientific, procedural, factual, and legal aspects. Its status determines its weight and fate. Factors determining its relevancy include lab accreditation, scientist qualifications, logical relevancy, legal relevancy, custody, and observed slander. If all the conditions are fulfilled then forensic evidence accepted as substitute to ocular account.

RELEVANT CASE LAWS

(M. Arshad vs, Sughran Bibi, 2008), petitioner filed a suit for maintenance, but later shorn of the legitimacy of his minor son. The domestic courts discharged his application, and he later appealed to the LHC. The court highlighted the importance of child's legitimacy and lined that a child who was born within the period of a lawful wed is legitimate. petition got dismissed, and he held liable for maintenance of child. Addition to this, Petitioner (Sharaf Ali Ashraf, 2008), filed a marriage jactitation suit after a daughter was born during the proceedings. The domestic special court decided in favor of the respondent and infant daughter, and the SC found that the evidence supporting the lawful marriage. Ashraf failed to prove the invalidity of the wedd and the legitimacy of the infant, who was born within the period and held lawfull. The court simply released Ashraf's petition, stating it was found to to escape his responsibility which is against sharia law.

(Azeem Khan and others v. Muhammad Khan and others, 2016), SC held that without supporting evidence DNA test cannot be reliable soly and considered it to be not admissible with expert evidence, citing the PFSA 2007 and QSO, 1984. Another case, (Shujaat Ali vs State, 2008), The court denied bail to Shujaat Ali, a petitioner accused of allegedly filming and distributing a video of his classmate's daughter's bathroom experience. The defense argued that Ali was falsely implicated due to procedural errors and lack of evidence. However, the court found that Ali had gathered evidence from an Internet Company, linking him to the crime. The investigation found electronic devices, including a CD containing the video, at Ali's behest. The court found no malicious intent in implicating Ali. The court noted the serious nature of the offense and the exceptions under Section 497 of CrPc, bail was deprived of. The Indian Supreme Court clarified that recording through tape does not fall under the category of proper evidence. (The State vs. Ahmed Omar Sheikh , 2021).

The Lahore High Court has ruled that mobile SMS records, under Article 164 of QSO 1984, are measured to be strongest evidence, and it can be qualify as chief evidence for legal rulings (Shafqat Masih vs. The State , 2021). The case of Ishtiaq Ahmed Mirza Vs Federation of Pakistan (PLD 2019 SC 675) emphasized the importance of forensic examinations and tests in determining the authenticity of audio tapes and videos. The advancement of science and technology has made it easier to edit, doctor, or tamper with audio tapes and videos, making it more unsafe to rely on them as evidence in court.

The case involved a media briefing by Maryam Nawaz, the existing Chief Minister of Punjab, alleging that Judge Muhammad Arshad Malik confessed to being pressured into a verdict. The controversy escalated, leading to petitions and the formation of an Inquiry Commission as per suggestion of Attorney-General, but the ongoing (FIA) inquiry was emphasized. The key issues identified were addressing the relevant video, establishing it as genuine evidence, proving it before a court, determining its effect on Nawaz Sharif's conviction, and addressing Malik's conduct. The case of Asif Ali Zardari and another Versus State (PLD

2001 SC 568) highlights the importance of digital evidence in establishing judicial delinquency. It highlights the need for forensic reports and legal procedures to maintain credibility and fairness in Pakistani courts. This is not safe to solely rely on evidence beyond a doubt and once the doubt on any evidence (video authenticity) it may destroy its credibility.

CONCLUSION

DE is rapidly evolving, aiding law enforcement in investigating and prosecuting crimes. It includes GPS data, text messages, photos, and more. However, challenges include inadequate resources, lack of training, and civil liberty concerns. Forensic science protocols are essential tools for crime investigation, complementing investigators' expertise. They facilitate investigations of murders, rapes, accidents, and cases involving anonymous bodies, missing persons, fraud, and forgery.

RECOMMENDATION

To improve the handling of forensic and digital evidence, it is essential to expand training programs for all law enforcement agencies, educate judges on processing and extraction techniques, need officers with evidence-handling ability, improve prioritization and preservation of modern evidence, and address apprehension concerning the prevalence of training and equipment for digital forensic inspectors. This will help streamline workflows, reduce unnecessary data extraction, and ensure proper evidence handling. Additionally, establishing additional forensic laboratories and providing comprehensive training for all stakeholders is crucial for ensuring proper forensic procedures in crime investigations. Investing in forensic technology, such as proof-collection kits, UV flashlights, laser-based measurement devices, safety suits, fingerprint development supplies, gunshot residue kits, blood stain detection kits, treatment, and lighting equipment, is also crucial for law enforcement agencies in remote areas.

REFERENCES

- Arshad, H., A. B., & O. I. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *journal of information processing system* , 346-376.
- Azeem Khan and others v. Muhammad Khan and others, 2016 S C M R 274 (2016).
- Bartlett v Smith, , [1843] 11 M. & W. 483 (EXCHEQUER OF PLEAS (ENGLAND & WALES) May 10, 1843).
- Casey, E. G. (2011). The growing impact of full disk encryption on digital forensics." Digital Investigation 8, no. 2. *ScienceDirect.com* , 129-134.
- ET0. (2002).
- Goodison, S. E. (2015). *Digital evidence and the US Criminal Justice System. Identifying technology and other needs to more effectively acquire and utilize digital evidence.*
- Gumbley v Cunningham, (1988) QB 170 (1988).
- Hameed, U., Z. Q., & K. Q. (2021). Admissibility of Digital Evidence: A Perspective of Pakistani Justice System.
- Homem, I. (2018). Advancing automation in digital forensic investigations. *phd diss, Department of Computer and Systems Sciences* . Stockholm University.
- HOP. (2016). *Digital Forensics and Crime*. Retrieved February 7th , 2025, from UK Parliament: www.parliament.uk/post

- Iqbal, M. (2018). *The Qanun-e-Shahdat* . Lahore: PLD Publishers.
- Karim, J. (. (2020). “*Access to Justice in Pakistan*” (Ch. 21) p. 540. Pakistan Law House ; Edition: Second.
- Khan, J. (. (2005). *Cyber Laws in Pakistan*.
- Khan, J. K.-u.-R. (1993). , *Principles & Digest of the Qanun-e-Shahadat, Commentary adapted from Justice Monir’s Principles and Digest of the Law of Evidence (Vol.1, Ch.3), p. 228. . Lahore, Pakistan: P.L.D. Publishers, 1993.*
- M. Arshad vs, Sughran Bibi, PLD 2008 Lah 302. (2008).
- Mukasey, M. B., J. L., & D. W. (2008). *The NIJ special report, electronic crime-scene investigation, a guide for 1st responder (2nd ed)*. Washington, DC 20531 : U.S. Department of Justice office of justice programs.
- NIJ. (2008). *electronic crime-scene investigation, a guide for 1st responder (2nd ed)*. Washington, DC 20531: NIJ, National Institute Of Justice.
- Prabhas C. Sarkar. (1913). *Sarkar’s Law of Evidence (13th edition) P. 46- 47. .*
- QSO. (1984). Article 131.
- QSO. (1984). Article 164.
- QSO. (1984). Article 2 (e).
- QSO. (1984). Article 2.
- QSO. (1984). Article 48.
- QSO. (1984). Article 59.
- QSO. (1984). Article 78-A.
- Salman Ahmad Khan vs. Judge Family Court, Multan, 2017 PLD 698. (2017).
- Shafqat Masih vs. The State , 2021 MLD 1415 (2021).
- Sharaft Ali Ashraf, 2008 SCMR 1707 (2008).
- Shujaat Ali vs State, MLD 2008 Lah. 467 (2008).
- State v Benner , [1874] 64 Me. 283 (1874).
- The State vs. Ahmed Omar Sheikh , 2021 SCMR 873 (2021).
- UNODC. (2021, September). Retrieved from <https://www.unodc.org/dohadeclaration/>
- Wahab, I. (2024). *Ocular evidence vs Medical evidence*.
- Wigmore, J. H. (1923). *A Treatise on the Anglo-American System of Evidence (2nd edition 1923, Vol. i), pp-32-33.*
- Zahoor, R. W. (2022). Digital Evidence and its Admissibility under Pakistani Law. *Zahoor, R., Waqar Khan Arif, S. M., & Bannian, B. (2022). Digital Evidence and its Admissibility under Pakistani Law. Journal of Development and Social Sciences, 3(4) , 51-60.*