P-ISSN: 2709-6254	Journal of Development and Social Sciences	Oct-Dec 2022, Vol. 3, No. 4
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2022(3-IV)06	[51-60]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Digital Evidence and its Admissibility under Pakistani Law

[1]Dr. Rashida Zahoor* [2]Dr. Sardar M.A. Waqar Khan Arif [3]Bushra Bannian

1. Assistant Professor of Law, Baha Uddin Zakariya University, Multan Sub-Campus Vehari, Punjab, Pakistan & Post-Doctoral fellow International Research Institute, Islamabad, Pakistan
2. Assistant Professor of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan
3. Lecturer of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan

***Corresponding Author:** rashidazahooradv@gmail.com

ABSTRACT

Digital evidence is much important in current modern world due to its diversity, accuracy and complexity. The world is agreed upon the point of admissibility of digital evidence, as enlightened from the domestic and international legislations, from one hand, the laws are presuming the digital evidence as admissible piece of evidence, on the other hand they directed every authority, not to negate the admissibility of digital evidence, merely on the ground that it is not in the form that is substantive and tangible in nature. In this context, this paper analyses the admissibility of digital evidence from the perspective of Pakistani law. It discusses the historical background, legislation on the subject and its presentation before the Court at the national level. The research methodology used in this paper is analytical. Relevant laws on digital evidence are analysed.

KEYWORDS Admissibility, Digital Evidence, Evidentiary Value, Legal System, Pakistani Law

Introduction

Digital evidence is defined as, evidence that is not in substantive form, means the kind of evidence is not tried by using formal methods of investigation, this is the most perishable and fragile evidence among all kinds as far as the definition of digital evidence is concerned it refers to evidence that is not in tangible form (NIJ Report). In today's world Computers are being manipulated for commission of offence like computer related fraud, identity theft, sending of spams and computer related solicitation etc. It is a well-known phrase that "iron cuts iron" here it means that now the law enforcement agencies utilize computers to fight computer generated crimes that are commonly known as cybercrimes.

Digital/ electronic evidence is basically information gathered or communicated in binary form that may be produced before the court and the court may relied upon such piece of evidence (The Doha Declaration). It has several places from which one may collect like it can be found on a computer hard disk, a mobile/cell phone, a Compact Disk (CD), and a pan derive etc. Digital evidence is generally connected with electronic crime (e-crime) such as fraud, committed through Automated teller Machine (ATM), child pornography hacking etc.

Historical Background and Literature Review

Forensic science is a reaction to a demand, reasonable care and diligence from the law enforcement agencies. It was early 1984, when the Federal Bureau of Investigation, an American based intelligence agency (FBI) and rest of other law enforcement entities started formulating the programs to study the computer evidence/electronic evidence. To address the issues/demands of investigation agencies and prosecution in organized and programmatic style, the FBI primarily established the Computer Analysis and Response Team (CART) though CART is specialist and professional in the FBI, its tasks and general

organization, it has demanded cooperation from other law enforcement agencies working in the United States (US) as well as the law enforcement agencies of other countries.

The primary problem highlighted and addressed by law enforcement agencies was categorizing the resources available within the group that could be utilized to inspect and examine the computer evidence/electronic evidence. These resources were frequently sprinkled throughout the agency now it's the time to move and utilize these resources and examinations to a cordoned off laboratory environment.

In 1995, when first survey was conducted by the United States of America (U.S.A) .Secret Service agency and highlighted that forty eight percent agencies had their own Digital forensic laboratories and sixty eight percent of evidence that is digital in nature has seized/taken-up was transferred to the experts working there in those laboratories. The aforementioned survey encouraged as the statistics came after survey, indicated a controlled progress to digital evidence and digital forensic needs. The same survey reported a shocking fact that about seventy percent of law enforcement entities are progressing without any standard law-making, guide or established standards.

Computer Forensics and Digital Evidence

In 1990, when the Postal Inspection Service Laboratory transformed to a brand-new facility at Dulles, Virginia, and by 1996-97, established of a Computer Forensic Unit occurred there. The Inspection Service committed to work diligently with FBI and passed several years in the formulating computer forensic abilities. On one hand all the agencies joined hands to establish a standard for digital evidence but on the other side, at about the same time, an important issue emerged which was audio and video enhancement from analogue to digital format, here the question raised that the same principles and standard be applied on the current issue, or the agencies travel more to find out a new way. Should the same guiding principles be applicable to all kinds of electronic evidence regardless of the output? Can inclusive "Digital Evidence Unit" (DEU) be more adoptive than a "Computer Forensic Unit" (CEU)?

The grand achievement is happened when Federal Crime laboratory's (FCL) directors arranged sitting twice a year to discuss the issues of common interest at Washington. They planned to establish what is known as the Scientific Working Group on Digital Evidence (SWGDE). At the early stage the casual definitions of digital evidence and forensics were given as "digital evidence is hidden evidence on a computer" and the concept of discovering them was termed as computer forensics at that time. On 2nd of March, 1998 the idea of digital evidence (included digital audio and digital video evidence) was taken before the federal laboratory directors, at a sitting conveyed by the Postal Inspection Service of US Forensic and Technical Services Division, Virginia and Dulles. The issue that was primarily discussed was digital photography (includes images, snaps in digital format). The discussion about digital evidence was certain but, opinion is given that digital computer or electronic evidence, digital audio and video, required technical/related people to chair and lead the discussion (Tubrazi, 2017).

A second sitting, followed by first meeting was held on 12th May, 1998, it was the first time when the directors accompanied with their technical staff to discuss ahead the technical merits and demerits of digital evidence. Dr. Don Kerr, (Assistant Director), FBI Laboratory, called Mark Pollitt, (Unit Chief) FBI's Computer Analysis and Response Team, to continue the discussion and enlighten the concept of digital evidence in front of the staff available there in meeting (Kerr, 2007). Scott Charney, chaired the Department of Justice, Computer Crimes and Intellectual Property Section (CCIPS) of US, was requested to highlight legal perspective of digital evidence and to enlighten the process through which one could seize digital evidence. This meeting gave fruitful results and contributed to development of new Technical Working Group to deal with forensic issues and used abilities to sort of them.

Irrespective of all the meaningful meetings the point of examination standards was unaddressed but in 1991 a joint sitting, of six international law enforcing agencies and US federal law enforcement agency hosted by US in South Carolina, the only minute of the meeting was to discuss frequently the standards for examination of digital evidence and computer forensics. In 1993, the FBI conducted a meeting called International Law Enforcement Conference on Computer Evidence, it was attended by seventy representatives of the U.S law enforcement (state and local law enforcing agencies) all the participants are agreed to formulate standards for computer forensic in order to address the issues of digital evidence. This conference was again called in 1995 which was hosted by Baltimore and Maryland, Australia hosted the same in 1996, and Netherland in 1997 a grand development happened and ultimately International Organization on Computer Evidence (IOCE) was established.

On June 17, 1998, (TWGDE) held their first Meeting. Mark Pollitt, Special Agent, FBI, was elected Chair and Carrie Morgan Whitcomb, Manager, Forensic Services, U.S. Postal Inspection Service was elected Co-Chair. Federal forensic laboratories that were represented included the Bureau of Alcohol, Tobacco and Firearms (BATF), U. S. Customs, the Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA), U.S. Secret Service (USSS), and the U. S. Postal Inspection Service. TWGDE met monthly to prepare organizational procedures and develop relevant documents. Mark Pollitt gave many international presentations to groups such as the International Organization on Computer Evidence (IOCE) and International Criminal Police (ICPO) INTERPOL (concerning the work of TWGDE (Whitcomb, 2012).

Scientific Working Groups (SWG): Replacement of TWG

The groups working in forensic science, evolved into the groups of experts in a distinctive discipline and gradually converged into specific bodies with specific features that formulate the standards, best practices, and protocols. They started their journey with a name "Technical working group" in 1990 that was renamed as "Scientific working group" in 1999, their work was distinctive in nature, and they were supported by both law enforcement and civil bureaucracy.

The first meeting of SWG was framed to deal with modern technological issues of forensic science, deoxyribonucleic acid (DNA) (Report NIST). It was named as Scientific Working Group for DNA Analysis Methods (SWGDAM), the step was itself indicated the reasonable development in the field of digital evidence and modern forensic science.

The results were clear regarding the establishment of a criteria/framework for operative rules and by-laws for the SWGs. The formulation of SWG was a matter of need of that time, it evolved day by day and now effective by-laws are needed to efficiently implement and execute the deliberations of SWGs, and it is important to mention here that each SWG formulate written by-laws for their operation. Although not every SWG can or should be covered by present standardized rules, certain standards of performance that are common to all SWGs were useful for consideration.

Processes have been developed by SWGs to gain input from non-members on proposed guidelines and procedures before finalizing such documents. In February 1999, TWGDE was changed to SWGDE. The Scientific Working Group Image Technology (SWG-IT) is closely associated with SWGDE and was originally part of SWGDE. For example, the taking of d digital pictures of evidence at a crime scene is digital imagery. When the digital picture itself is the evidence (as in the case of child pornography), it would be digital evidence and part of SWGDE.

As SWGIT develops enhancement protocols, there is much commonality between the two SWGs. The mission of the Scientific Working Group on Imaging Technology (SWGIT) is

to facilitate the integration of imaging technologies and systems in the criminal justice system by providing definitions and recommendations for the capture, storage, processing, analysis, transmission and output of images (SWGIT, 1999).

The Digital Evidence and its Admissibility: Legal framework in Pakistan

As it is primarily described in the early chapter of this research that digital/electronic evidence is now admissible evidence in rest of the world, the criteria mechanism may differ from state to state but the point of admissibility is very much clear. Unlike other states Pakistan also tried to make amendments in law of evidence as per the needs and demands of trends set by the modern world and enacted several laws in order to complement the laws with the trends set by I.T, main contributions includes, the amendment (addition of some Articles and addition of some provisions in the existing Articles) in Qanun-e-Shahadat Order, 1984, promulgation of Electronic Transaction Ordinance, 2002, The Prevention of Electronic Crimes Act, 2016, Investigation for Fair Trial Act and Rules, 2013, Federal Investigation Act, 1974, Anti-terrorism Act, 1997 etc.

The Qanun-E-Shahadat Order, (1984) and the Digital Evidence

The Qanun-e-shahadat Order, 1984 (QSO) is basically an Ordinance promulgated in the times of Gen Zia Ul Haq, the man tried to insert the provisions of Islam in the Evidence Act. 1872. The preamble of the Order is very much clear about the essence of its promulgation, it was promulgated to revise, amend and consolidate the law of evidence so as to bring it in conformity with the injunctions of Islam as laid down in Holy Quran and Sunnah (The QSA, 1984 Preamble). The Law of Evidence was available before this promulgation and given by British India Government before partition of subcontinent, as the evidence from one side is the formal transaction but Islam gave it a spiritual covers. In Islam the term evidence is some kind of sacred transaction, is explained in Quran in Surah-e Nissa and Sura-e-Maida and highlighted in Sunnah. As far as the admissibility of digital evidence from the source of QSO, 1984 is concerned, the legislators added some new Articles and made some additions in the available Articles. Article 2(e) is incorporated through which the digital terms as introduced by ETO are adopted. Article 48(a) is another amendment brought in QSO, 1984 through which the information generated, received or recorded by automated information system became relevant.

An amendment was brought in Art-59 QSO 1984, such as, "opinion of expert" thereunder some words and expressions are added like "authenticity and integrity of electronic document made by or through an information system", "Functioning, specifications, programming and operation of information system, are relevant facts." Article 78-A of QSO, 1984 is also an amendment brought to address proof of electronic signature and electronic document. It describes that if an electronic document is made completely or in part or signed by using information system and when such fact is negated, the security procedure to sign or electronic document must be proved. Article 164 is also incorporated which is "production of evidence that has become available because of modern devices etc." through this Article the legislators confirmed that the court may allow to, produce any evidence that is available because of the modern devices and techniques. The convictions imposed by the judge on the basis of the electronically generated evidence is also legal (Criminal Amendment Act, 2017).

Electronic Transaction Ordinance, (2002)

The Electronic Transaction Ordinance, 2002 (ETO) came with the objective that the electronic/digital evidence is the admissible piece of evidence, it cannot be denied as admissible piece merely on the ground of having digital shape, the Preamble of this Ordinance clearly indicates its purpose of enactment as sufficiently endorsed in its name "an ordinance to recognize and facilitate the documents, records, information, communication and transaction in electronic form and to provide for accreditation of certification service

providers" (ETO, 2002). The preamble is multifunctional though main of its part is from the conventions proposed and passed by the UN but the thing that really matters is the legislation in a country, unlike other countries Pakistan tried to complement the law of evidence (QSO, 1984) though making amendments in it and by enacting these sorts of laws. The ETO is comprised of VI Chapters and 51 Sections.

As far as the theme available in the preamble of ETO, 2002 is concerned it is multidimensional and multifunctional, in the start of the preamble the legislature made one thing clear that the purpose of its promulgation is to recognize, here it means that the evidence that is available in digital format is to be recognized on every forum, the complementary portion continued with "and facilitate" here it means the other prime concern of this promulgation is to facilitate the admissibility of the evidence available in digital/electronic form and to demolish the hurdles available in its legal way. The upcoming portion describes the form of evidence, means every possible mean whether the digital evidence is in the form of documents, records, communication, audio and etc. it would be admissible and can be brought before the court of law as a piece of evidence. At the end it is providing accreditation for certification service providers, here it means that the digital evidence while brought before the court of law is accompanied with its certificate of its authenticity and veracity, so the court rely on it and consider it as a piece of valid evidence in proceeding.

After the amendment in QSO, 1984 the ETO is considered on top while we are talking about the digital evidence and its admissibility. The ETO is enriched with the best practices of the electronic/digital evidence in routine life like on one side it is recognizing the presence of digital evidence and on the other hand it directs the authority to consider the digital evidence in the court proceedings and do not negate it solely on the grounds that the evidence is available is in the digital format. The ETO, 2002 is against the corroboration of the digital evidence by the formal witness or evidence, It is observed in previous years that the court consider the digital evidence if it is corroborated by the formal witness, but if it is not complemented by the witness it was negated and neglected, the provisions of ETO are clear on this point that the digital evidence if having the authentication certificate with it need not to have a witness behind it to corroborate the same before the court of law.

More importantly the ETO, 2002 concerned with the electronic transactions. Electronic transaction hereby means the transactions in digital format like digital records, digital communications etc. The world is now replacing the formal transaction by digital/electronic transactions, so the electronic transaction is need to be clarified, need the electronic/digital evidence to be proved before any legal forum so the promulgation is having prime importance in Pakistan because it defines and recognizes the evidence that are in digital form from each perspective and recognizes the same and gives a brief account of electronic transaction which is having special importance in the whole world.

The ETO, 2002 is considered as the landmark in the mainstream of digital evidence, cybercrimes, digital forensics, and digital investigation. It is complete in its premises but where it lakes something, the QSO, 1984 is there on its back to complement it from four ends, the prime characteristic of this promulgation is that it is a multidimensional law (ordinance) that on one side describe the possible digital offences/cybercrimes but also empowered an agency to conduct investigation, from other dimension it gives a brief account of the principles upon which the investigation is conducted, this piece of promulgation strengthen the validity and admissibility of digital/electronic evidence and clearly states that the digital testimony must not be neglected as a reliable piece of evidence merely on the ground that it is in electronic/digital shape, it changes the trend of further/corroboratory evidence for admissibility now the digital evidence need no corroboration, it is now practiced and considered as a reliable piece of evidence.

Digital Evidence: On Presentation before the Court

The definition of evidence and its kinds are well explained in the previous chapter of this work, as far the valid digital evidence is concerned, there involve a procedure by which the digital evidence mended and enabled to be presented before the court of law (UNDOC, 2019). The process by which the expert amends the evidence, transform it into a shape, that is presented before the court of justice during the trial along with the report of its varsity is said to be digital forensic. It is now the world's need to complement the laws of digital evidence and digital forensic from each side, and to cope the loopholes available in the laws that have already been enacted by passing amendments.

Digital offence is replacing the formal offence in this modern time, the offenders are now manipulating the computer and rest of other digital devices to commit offence because the concept of crime/offence is now having no territory, the crime is now borderless and is most dangerous as compared to formal offence. Digital Evidence is as brief as the admissible piece of evidence like other evidence such as substantive evidence e.g. cloths, dagger, gun, swabbed fabric, documents etc. but there in case of digital evidence the values and standards, from the beginning differ from the substantive evidence. The initiative could not be taken without the scientific knowledge and expertise because the fragility in this perspective is so obvious, the whole crime-scene could be vanished by a mistake, and it is the job of the investigator to apply its knowledge and expertise to deal with the digital evidence and to give it a shape which is being admitted in a court of law during a legal proceeding. Another salient feature of the act under consideration is that it provides a complete mechanism of execution of warrant, the acts that could be done during execution like recording telephonic communication, video recording of a person etc (The investigation for fair trial Act, 2013 s 16 to 21).

The job of law enforcement agencies started on the commission of an offence, like in Pakistan the Police is the investigation agency (The department of police is established under (Police Act, 1861 s 2). The Police Act, 1861 established the department with two main functions one is, to deal with law enforcement and the other is to investigate the crime/offence, these two functions are eminent in the police of the entire world. The police after registration of case under the law starts collecting evidence. The investigation in simple words is defined as the collection of evidence by the police, after completion of investigation the police is duty bound to present the report of investigation (*Challan*) before the court of law through public prosecutor after that the trial begins (Criminal procedure code, 1898 s 173). There are two kinds of trials in Pakistan, one is the trial before the Magistrate and trial before the Court of Session. Trials before either court has common steps, the trial before the Magistrate dealt under Chapter XX of Cr.Pc. The trial before the Curt of Session dealt in Chapter XXII-A of Cr.Pc (CrPc 1898, s 265 a to 265 n). When the trial begun in either court following process is to be adopted by both courts:

i. The trial begun through public prosecutor (CrPC 1898 s 265 a);
ii. Supply of statements and documents to the accused (CrPC 1898 s 241 (a) and 265 (c));
iii. When charge to be framed (CrPC, 1898 s 242 & 265 d);
iv. Plea (CrPC 1898, s 265 e);
v. Evidence from the prosecution (CrPC 1898, s 265 f);
vi. Summing up by prosecution and defense (CrPC 1898, s 265 g);
vii. Acquittal or conviction (CrPC 1898, s 245 & 265H);
viii. Procedure in case of previous conviction (CrPC 1898, s 245A-265I);
ix. Statement Under section 164 is admissible (CrPC 1898, s 244(a) and 265(j));
x. Power of the court to acquit the accused at any stage (CrPC 1898, s 249(a) and 265(k));
xi. Power of Advocate General to stay prosecution (CrPC 1898, s 265L);
xii. Time of holding sittings (CrPC 1898, s 265M); and
xiii. Place of holding sittings (CrPC 1898, s 265N).

There are two kinds of the criminal courts in Pakistan (CrPC 1898, s 6). The court has the symbol to adjudicate the matters and to administer the justice, and it is the job of law Investigation agencies to investigate the matters of digital evidence with efficiency and to present the facts truly before the competent court of law. The court is blind without fair investigation, the courts is dependent on investigation, if the investigation has fair basis than no one could protect the real culprits from the force of the law. The courts are not bound by law to decide the matters/cases merely on the basis of police report presented before it after completion of investigation by the police, the courts before considering a piece of evidence as admissible, tried to determine the authenticity (ETO, 2001) and veracity of the evidence by using several means, the court may by itself conduct inquiry to probe the fact and to determine its veracity if the court is satisfied from the report presented by police after investigation, it may decide the case on the basis of that report (CrPC 1898 s 117).

Digital investigation is totally different from casual investigation, as it is described in earlier chapters that the investigation of digital offences requires a person well-equipped with the knowledge, excellency and skill because digital evidence even from the beginning required the due care, a blink of negligence may vanish the whole crime scene. The investigator here uses due care, knowledge and expertise to cordoned off the crime scene and use the scientific devices and techniques to collect, transform, store and preserve the evidence, unlike the formal investigation where the investigator collects the evidence by using his hands, like collecting the dagger, the swabbed cloths, the blood stains, the ammunition and empties etc. the investigator of the digital offence uses the techniques, scientific methods, scientific means and devices, knowledge and skill to collect and process the digital evidence. After collection of the evidence in digital format the investigator processes such evidence through different scientific means to preserve and to shape it for presentation before the court of law for assistance, these processes may include, initiation and seizure of the crime scene and electronic evidence, make several copies of it for the next process, like digital forensic.

The role of the experts is also important in both formal and digital investigations, several laws, gave space to expert opinion as a reasonable assistance to the court like the UK criminal procedural rules enlightened the expert opinion (the expert where required to give opinion on a specific issue to help the court shall give unbiased opinion on matters by using his experience and expertise. These instructions are only given by the competent authority like a court or the authority to whom he may take his salary and it is the duty of an expert to give opinion whenever the court requires so. As far as the Pakistani law is concerned, the QSO gave space to opinion of expert in Chapter-III, Section 59 in these words: “when the court has to form an opinion upon a point of foreign law, or of science/or art, or as to identify of hand-writing or finger impression; the opinion upon that point of person specially skilled in such foreign law science or art, or in question as to identify of hand-writing or finger impression are relevant facts, such persons are called experts” (The Qanun e shahadat order 1984, art 59). From the above discussion it is evident that the opinion of expert has a prime importance in legal proceedings, the experts are the persons who assist the court by using their knowledge and skill, they are not the investigators, and their job is to assist the court where it requires their skill and expertise on a point related to their field.

As it is evident that the cybercrimes are more serious than the casual crimes like theft and robbery. Cyber offences manipulate the whole world, the whole world is not safe from cyberattacks, and one can see and compare the recent decade with current situation to find out the legislation on cybercrime and digital investigation. The standards are somehow proposed by rest of the countries, but no one claimed them as utmost because somehow every standard lacks something which is ultimately responsible for safe haven for cyber offenders, because the accused is a favorite child of law, and every shadow of doubt gives benefit to accused in criminal proceedings.

The provisions of the core legislation in Pakistan on the admissibility of digital evidence are crystal and clear, every law of the related field not only declare the digital evidence as admissible piece of evidence but is available to create the trend and to mold the legal systems of the world on a point where they admire the efforts. The process that really matters is the investigation. More durable and true is the investigation, more chances to execute the responsible offenders to evaluate the laws to meet the upcoming challenges. The admissibility of digital evidence is also dependent on the fair investigation, if the court makes opinion that the investigation that is being conducted by investigator is true, fair and unbiased, than the court freely rely on the investigation and decide the matters accordingly but whenever the investigation is not conducted on fair basis it results in doubts which are created during the trial by the lawyers and the courts acquit the accused by giving them benefit of doubt.

The apex courts of Pakistan are involved in proposing the new horizons and principle in the field of information technology and one of the massive threats to whole digital system is digital/cybercrime. From time to time the Supreme Court of Pakistan and High Courts adjudicate different cases and draw rules there to guide the law enforcement and forensic teems to follow the settled way. Supreme Court of Pakistan in his recent judgment declared that whenever a digital fraud is highlighted the investigation of that fraud can only be investigated by the department of National Accountability Bauru (NAB) (*(2019) PLJ Cr.C 71 (SC)).*

Another landmark judgment of the court clearly indicates that, the investigator and the prosecution are not limited to prove one guilty act by adopting the means of admissibility of digital evidence during a legal proceeding, they also need to prove the guilty mind behind the guilty act (*Rana Imran Latif v. State (2017) PLJ Cr.C 966 (Islamabad)*). The Lahore High Court in a judgment relied on the digital evidence presented before it by the investigation team in form of a report in a post arrest bail, the matter was about The Prevention of Electronic Crime Act, 2016 and FIR was lodged thereto, the court relied on the evidence brought by the investigative authority, instead of relying on his own discretion (*Usman bin Farooq v. State etc. (2018) PLJ Cr.C 58 (Lahore)*). The importance of this case is that the I.T experts aids the investigative authority in identifying and connecting the allegations by using his mobile phone data and I.P address.

Another judgment is important, which give the cooperative analyses of the evidence brought before the court during digital investigation, as whenever computer is used in collection of digital evidence is admissible piece of evidence as audio, video or any other information contained by the digital devices, the judgement is also a judgement that interpret the Art-164 of QSO, 1984 (*PLJ 2011 Sh.C-AJ&K 1*).

One of the important judgments on the admissibility of digital evidence is that the investigator needs to collect the evidence to corroborate what he obtained from the digital device likewise an audio call needs some more evidence to prove and identify the accused (*PLJ 2002 Cr.C 1421*). Another judgement passed by apex courts of Pakistan, while interpreting the nature and scope of Art 164 of QSO, 1984, there the court elaborate the scope and mentioned there that the digital evidence that in recent time produced is due to digital devices that are being used in digital investigation and forensic examination, the court briefly described, what can be brought before the court as admissible digital evidence, the court enumerate the cell phone, memory cards, audio, video etc. these all are admissible pieces of evidence if during the forensic examination the authenticity is being proved (*Yasir Ayyaz etc. v. State etc. (2019) PLJ Cr.C 352 (Lahore)*).

Conclusion

In Pakistan, even though the Digital evidence is the piece of evidence, which is admissible as evidence, in the legal proceedings. The evidential value of this, is not something definite and is to be corroborated by other substantive evidence that is available

on the record. The classification and the category of digital evidence is also uncertain and unsure, many debates are conducted on the said matter. To give space to the digital evidence as admissible piece of evidence, the parliament of Pakistan passes amendments in QSO, (1984) and another law which enlighten the stance of Pakistan in this field is Electronic Transaction Ordinance, (2002), by taking the example of the court on the issue of admissibility of digital evidence during trial of the case one came to know that there is still some uncertainty about the evidentiary value of digital evidence. In practice, most of the courts still look for other evidence that is presented to corroborate the digital evidence, it is hard to see in practice that the court fluently relay on digital evidence.

References

Criminal Amendment Act (IV of 2017).

Criminal procedure code, 1898 s 2, s 117, s 154 to 155, s 173, s 241 to 250, s 265 a to 265 n.

Electronic Transaction Ordinance, 2002. Preamble, s 16(3) e, s 4 a.

Kerr, D., (2007). GEOINT Symposium, US Geospatial Intelligence foundation, Online at: https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20071023_speech.pdf (Last assessed 10 December, 2021).

PLJ 2011 Sh.C-AJ&K 1.

PLJ 2002 Cr.C 1421.

Rana Imran Latif v. State (2017) PLJ Cr.C 966 (Islamabad).

The NIJ special report, electronic crime-scene investigation, a guide for 1st responder (2nd edn) < www.ojp.usdoj.gov/nij> (Last accessed 08 December 2021).

The Doha Declaration promoting a culture of lawfulness (UNODC), computer related offences<https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html (Last accessed 08 January, 2022).

The investigation for fair trial Act, (2013) s 16 to 21.

The Police Act, (1861).

The Qanun-e-Shahadat Order QSO, (1984). Preamble, Arts. 2e, 78-A.

The UK Criminal Procedural rules, (2015).

Tubrazi, S. J. (2017). Law of digital forensic, Chapter 1, the evolution of forensic technology, March.

UNODC, use of digital forensic in counter terrorism cases < https://www.unodc.org/pakistan/en/use-of-digital-forensics-in-counter-terrorism-cases.html> (Last accessed 10 October, 2021).

Usman bin Farooq v. State etc. (2018) PLJ Cr.C 58 (Lahore).

Whitcomb, C.M., (2012). "An historical perspective of digital evidence: a forensic scientist view". I*nternational journal of digital evidence.* volume /issue 1.

Yasir Ayyaz etc. v. State etc. (2019) PLJ Cr.C 352 (Lahore).