Majallah-yi Talim o Tahqiq

Markaz Talim o Tahqiq, Gulshan-e-Taleem,
Sector H-15, Islamabad, Pakistan

مجلہ تعلیم و تحقیق

مرکز تعلیم و تحقیق، گلشنِ تعلیم، ایچ۔۱۵، اسلام آباد، پاکستان

ISSN (P): 2618-1355, **ISSN (Online):** 2618-1363

Issue 1,Vol 4,January-March,2022

شمارہ ۱، جلد ۴، جنوری—مارچ، ۲۰۲۲

DIGITAL EVIDENCE: TESTIMONY OF EXPERT WITNESS IN PAKISTANI LAW

Mahboob Usman[1]

Keywords:

digital evidence, expert testimony, forensic evidence, circumstantial evidence

Abstract:

The world is rapidly producing electronic gadgets which are capable of digitally connecting with other devices and leaving traces which can be used as substantiation. Information technology is moving too fast to an extent that prediction of future technology is not imaginable. Hence, the legislative bodies are unable to predict the technological developments and make laws proactively, therefore, legislations designed for a specific objective may fail when a new situation arises. Almost, every electronic device is leaving a digital trace which can be used as evidence in judicial proceedings. Consequently, preserving digital evidence require special procedures ought to be followed since its generation till final disposal. Without, properly understanding its unique characteristic, it is difficult to produce the same in judicial forums. Due to novel issues attached to the situation, digital evidence is examined by the forensic experts. This research aims to demonstrate the definitions of digital evidence in the judicial parameters to facilitate the experts and legal fraternity for better understanding of it and making use of the same for judicial purposes. The paper further examines the amendments made in *Qanun-e-Shahadat* Order 1984 through Electronic Transactions Ordinance 2002, with the purpose to measure the extent of application under these amendments. Thereafter, complications faced by the investigator while collecting the evidence is examined. At the end, the paper discussed the role of expert in the light of legal instruments and proposed amendments ought to be made in the legal system of Pakistan to accommodate the report of digital forensic expert to make it admissible judicial proceedings.

.

[1] PhD scholar at the Department of Law, Faculty of Shari'ah and Law, International Islamic University, Islamabad and can be reached through mehboob_usman@yahoo.com

I. INTRODUCTION

The world is full of digital devices and without them, society will probably collapse. Many devices "even the most innocuous device may contain information which is relevant in a criminal investigation."[2] Therefore, it is stated that "a criminal action of an individual cannot occur without leaving a mark,"[3] or evidence, which is helpful in tracing out the criminal. Thus, it can be said that the evidence is the most important thing in investigation and prosecution. Whereas evidence in "its purest form is information presented in testimony or in documents that is used to persuade the fact finder to decide the case for one side or the other."[4] While the electronic[5] evidence is the "information and data of investigative value that is stored on or transmitted by an electronic device."[6] Such evidence is "acquired when data or physical items are collected and stored for examination purposes."[7] The definition of evidence is found in the Pakistani legal system, however, electronic evidence is not defined anywhere in existing laws.

Every day, without realizing we create digital evidence by using different devices, whenever someone operates his computer, surfers the internet, plays online games, makes a phone call, writes an e-mail, or writes a document, takes a ride while using the GPS unit, takes a picture or makes a video by using digital cameras, web cams, or shops online or pays online bill, all such devices generate some type of digital evidence. Even the copy machine, fax and scanner also contain digital evidence. Moreover, as we see every day, that the CCTV cameras are also an important source of digital evidence. In addition to this, credit card and debit card also contain digital evidence. Recently, installed traffic enforcement cameras are also a source of digital evidence creation, which capture the license plate number and e-challan is directly sent to the vehicle owner.

Nowadays, no device is protected from creating or storing digital trace that can somehow be used as evidence, and this can be found on everything "from floppy disks to media cards, solid-state memory sticks, solid-state hard drives, cell phones, network attached storage devices, game consoles, media players, hard drives, and the Internet cloud."[8] In existing regime, various online backup services are available, therefore, many people are using these services to store their data. Thus, it is becoming more challenging for the investigator to "track down where all the data might reside in a forensic case... [Furthermore,] there are now many applications and storage options available through such services."[9] Another source of digital evidence creation is social media, which records the activities of users including personal information, location and thought of the user. Likewise, several social applications and chatrooms are also source of digital evidence. Consequently, we can safely conclude that digital evidence is everywhere.

---

[2] Angus Marshall. *Digital Forensics Digital Evidence in Criminal Investigation* (Willey-Blackwell, 2008), ix.

[3] Richard Boddington. *Practical Digital Forensics* (Birmingham: Packet Publishing Ltd., 2016), 3.

[4] Albert J. Marcella and Doug Menendez. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. 2nd ed.* (New York: Auerbach Publications, 2008), 11.

[5] Also referred to as digital evidence.

[6] Ibid.

[7] Ibid.

[8] Larry E. Daniel and Lars E. Daniel. *Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom* (New York: Elsevier, 2012), 5-6.

[9] Daniel et al. *Digital Forensics for Legal Professionals*, 6.

The fast advancements in virtual world occurring in existing regime of information communication technology is presenting new challenges to the investigators, making digital evidence difficult to detect, preserve and produce before the courts, therefore, there is dire need to understand and examine the existing legislation on the subject. In Pakistan, first ever legislation on electronic subject was "Electronic Transactions Ordinance, 2002,"[10] (ETO) and the basic purpose of the ETO was "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."[11] This Ordinance also amended few provisions of the *Qanun-e-Shahadat* Order, 1984 (QSO).[12] The provisions of this Ordinance were used to cover many aspects of cyber-crimes till 2016. Although, during the trial many of the criminals were acquitted due to non-applicability of the Ordinance, hence this Ordinance was not sufficient to cover many aspects of cyber-crimes particularly digital evidence. However, the Prevention of Electronic Crimes Act, (PECA) 2016 strengthened the LEAs by extending the international cooperation for investigation purposes,[13] which is a good step to enhance the powers of LEA. Thus, LEA will be able to collect evidence from other countries. QSO was made in 1984, when nobody has foreseen future of evidence, especially on computers as the first windows was introduced in 1985.

Digital evidence is not like conventional evidence,[14] as in conventional evidence all stages from identification to production before the court is easy task but in the case of digital evidence, it is difficult for expert witness to handle the situation, therefore, he has to make maximum efforts for all stages of the evidence. Generally, preserving the crime scene is the primary objective of the investigator because "if the evidence is contaminated, lost, or simply not identified and overlooked, then all that follows may be of limited value to the investigators putting together the case evidence."[15] However, in digital evidence it is not a piece of cake for the investigator to preserve digital crime scene, making more difficult the job of expert witness. Various procedure are involved in this process, as "evidence cannot be viewed in isolation and should be compared with other evidence, and corroborating evidence should be identified."[16]

The main issue with digital evidence is that "it is actually just a collection of ones and zeros represented by magnetization, light pulses, radio signals or other means. This type of information is fragile and can be easily lost or changed."[17] Whereas

> protecting the integrity of evidence and maintaining a clear chain of custody is always important in a criminal case, but the nature of the evidence in a cybercrime case makes

[10] Electronic Transactions Ordinance, 2002 (LI of 2002).

[11] Ibid., Preamble.

[12] The *Qanun-e-Shahadat* Order, 1984 (P.O. No. 10 of 1984).

[13] S. 42 of Prevention of Electronic Crimes Act (PECA), 2016.

[14] Chapter X of the QSO, 1984 provides the detail procedure for examination of witnesses. Chapter XL and XLI of the Code of Criminal Procedure, 1898 provides for the commissions for the examination of witnesses and special rules of evidence. Under CPC, 1908, the High Courts have been granted power to make rules for their respective provinces. Thus, for civil matter rules are framed under CPC to tackle evidence which are normally called Orders. Order, 11 (discovery and inspection), 13 (production, impounding and return of documents), 16 (summoning and attendance of witnesses), and 18 (examination of witnesses) are relevant for this study.

[15] Boddington. *Practical Digital Forensics*, 5.

[16] Ibid.

[17] http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed on 5th July 2017).

> that job far more difficult. An investigator can contaminate the evidence simply by examining it, and sophisticated cybercriminals may set up their computers to automatically destroy the evidence when accessed by anyone other than themselves.[18]

In many situations, if the compromised system is not adequately secured than it will be very challenging to determine or prove an allegation against the culprit, as since someone else can hack into a system without the authorization of the lawful user. In some cases, criminals may remove logs to hide what happened, "so that there is no evidence to prove that a crime even occurred."[19]

As the subject of digital evidence is new thus only "few people are well versed in the evidential, technical, and legal issues related to digital evidence and as a result, digital evidence is often overlooked, collected incorrectly, or analyzed ineffectively."[20] This is the situation in the developed countries. However, the developing countries are far away from accepting this demand. It is so powerful that it can "reveal communications between suspects and the victim, online activities at key times, and other information that provides a digital dimension to the investigation."[21] The topic of digital evidence is extensive, and it covers "diverse issues ranging from the collection, storage, and preservation to the authentication, validation, and application of electronic evidence, and raising questions on privacy, cost, ethics, and procedural management."[22] With the passage of time, devices containing digital data may "deteriorate over time or when exposed to fire, water, jet fuel, and toxic chemicals."[23] While examining, interpreting and presenting digital evidence certain errors can be introduced, complicating the job of investigators more difficult.

II. DEFINING DIGITAL EVIDENCE

Different terms have been used for defining and describing digital evidence including electronic and computer evidence. All these terms definite some features of digital evidence. Yet, "defining what these distinguishing features are is far from straightforward."[24] As the fast growth and changes in Information Communication Technology (ICT) may make any definition obsolete. The use of digital evidence has increased exponentially since last few decades. There is no uniformity in use of terms. Both terms (electronic and digital) are globally used by the scholars and legal fraternity. Besides, there are various definitions of "digital or electronic evidence." However, every definition highlights some important features. Simply stated, digital evidence is any kind of evidence that comes in digital form rather than to paper

[18] Ibid.

[19] Ibid.

[20] Eoghan Casey, *Digital Evidence and Computer Crime*, 3rd ed. (New York: Elsevier, 2011), 8.

[21] Casey, *Digital Evidence and Computer Crime*, 16.

[22] Xandra Kramer, "Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise," *Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL*, XXVI (2018): 391-410 at 393.

[23] Casey, *Digital Evidence and Computer Crime*, 27.

[24] Stephan Mason and Daniel Seng. *Electronic Evidence*. 4th ed. (London: School of Advanced Study, University of London, 2017), 19.

or any tangible form. There are various, worldly, accepted definitions which have been provided by different organizations and scholars. The followings are some of the definitions:

The Scientific Working Group on Digital Evidence (SWGDE) defined digital evidence as "any information of probative value that is either stored or transmitted in a digital form."[25] While the International Organization of Computer Evidence (IOCE) defined it as "any information stored or transmitted in binary form that may be relied upon in court."[26] However, these definitions "focus on proof in court and neglect data that can make an investigation advance further. That the term binary is inexact describing just one of many common representations of computer data."[27] This term is no more in use and SWGDE changed the term "binary" with "digital" to include digital audio, video, cell phones, and digital fax machines.[28] Eoghan Casey[29] proposed the following definition that digital evidence is "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi."[30] Whitcomb has criticized this definition in the following words:

> Although the emphasis of this definition is on criminal investigations, it is a wider definition than the previous definitions, and it usefully explicates certain important aspects of electronic evidence. For instance, the reference to 'data' is to information that is held in electronic form, such as text, images, audio and video files. Also, the word 'computer' must be understood in its widest possible sense, and incorporates any device that stores, manipulates or transmits data. In addition, the definition implies that the evidence must be relevant and admissible, a question that can only be answered after we know what the electronic evidence, whether admissible or inadmissible, actually is.[31]

Definition of digital evidence by Casey is wider as compared to other definitions, proposed before him, as the word 'data' is to information means data which is held in electronic form and the word 'computer' is to be understood to its widest possible sense, *i.e.*, any device which stores, transmits, or manipulates data. The scholars Schafer and Mason[32] has proposed the following definition:

> Electronic Evidence is data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.[33]

---

[25] https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v2-8 (accessed: 9th August, 2018).

[26] The definition was adopted by IOCE in 2000.

[27] Casey, *Digital Evidence and Computer Crime*, 7.

[28] Carrie Morgan Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence* 1 (2002): n.d.

[29] Eoghan Casey is the author of *Digital Evidence and Computer Crime*, and coauthor of *Malware Forensics*.

[30] Casey, *Digital Evidence and Computer Crime*, 7.

[31] Mason and Seng, *Electronic Evidence*, 19.

[32] Stephen Mason *Barrister of the Middle Temple.*

[33] Mason and Daniel Seng. *Electronic Evidence*, 19.

According to the scholars Schafer and Mason this definition consists of three elements:

i. reference to 'data' includes "all forms of evidence created, manipulated or stored in a device that can, in its widest meaning, be considered a computer."[34]

ii. this definition includes "the various devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition will include any form of device, whether it is a computer as we presently understand the meaning of a computer, telephone systems, wireless telecommunications systems and networks, such as the Internet, and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems."[35]

iii. this definition restricts "the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes."[36]

The term digital or electronic evidence is not defined in Pakistani legal system. However, the term evidence is defined in QSO and the term electronic is defined in ETO and PECA respectively. The ETO defines the term electronic which includes "electrical, digital, magnetic, optical, biometric, electrochemical, wireless or electromagnetic technology."[37] Although, the PECA has adopted the same definition of the term electronic, but an additional word electromechanical has been made part of the definition, which provides that "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology"[38] and the term evidence has been defined which includes;

> (i) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; and
>
> (ii) all documents produced for the inspection of the Court; such documents are called documentary evidence.[39]

In Pakistani legal system, definition for digital evidence in not provided in any legal instrument. The existing law of evidence is only meant for the facts of physical world. Thus, on the basis of above-mentioned discussions, it can safely be concluded that it does not fulfill the purpose of a comprehensive and precise definition creating difficulties for the LEAs, Judiciary and other persons working on the field to understand the digital evidence as it ought to be. Instead of using the term 'electronic' the term digital evidence will be used throughout this paper.

III. MODIFICATIONS AND ADDITION IN QSO

In Pakistan, the previous law of evidence[40] was written at a time when information was used to be stored primarily on paper, in the form of documents and these rules were designated

[34] Ibid.
[35] Ibid., 20.
[36] Ibid.
[37] Section 2(1) (l) of the ETO.
[38] Section 2 (1) (xvii) of the PECA.
[39] Section 2 (1) (c) of the QSO.
[40] Evidence Act, 1872.

to deal with information stored on papers. Similarly, the existing law of evidence is not capable of addressing information stored in electronic forms. Astoundingly, Article 164 of QSO does not mention information stored in electronic form. After all, how can it be expected that a law primarily meant to deal with paper documents to function in a paperless world? Whether there was a need to modify QSO to impose severe requirements for the acceptance of computer related evidence. In 2002, first time in Pakistani legal history, need for amendment in QSO was felt to make computer-generated evidence admissible. Although, Article 164 of the QSO was there in the field. But being unable to handle the requirements of 21st century, a need was felt by the legislature to address the un-addressed issues. Therefore, the QSO was amended, and the following developments took place with the promulgation of ETO.

Article 2 of the QSO was amendment and two new sub-clauses namely (e) and (f) were added and the following expressions were given the meaning which were attributed in ETO. These expressions are automated, electronic, information, information system, electronic document, electronic signature, advanced electronic signature, and security procedure. And in sub-clause (f) the expression 'certificate' was defined. To provide for the admission of automated generated information, in Article 30 of the QSO, an explanation was added. Similarly, a new Article 46-A, for acceptance of electronic documents in evidence, was inserted in QSO. Expert opinion is integral part of Islamic Law and English common law. Thus, keeping in view the requirements of contemporary world, Article 59 of the QSO was also amended and few words were added and substituted to clarify the legal position. Moreover, printout was declared as primary evidence through the amendment of Article 73 of the QSO. Basic purpose of ETO was to recognize and facilitate electronic documents. Since, before the 2002, electronic signature was not accepted in Pakistani legal system. To recognize the electronic signature and documents, a new Article 78-A in QSO was inserted.

There are two types of documents public and private. Article 85 of the QSO deals with public documents. Keeping in view the requirement of business community, this article was also amended in 2002, and certificates deposited in repository was recognized as public documents. Afore discussed modifications which took place with the promulgation of ETO. Here question arises whether these modifications are applicable to all proceeding either civil, criminal, commercial or to the selected laws? As per section 29 of the ETO, all amended brought in the QSO through ETO are only meant for ETO and are not extended to other laws, instead of realizing this aspect, the courts, incorrectly, applied the same amendments in every case where some type of digital evidence was recovered. Thus, section 29 of the ETO be amended to apply amendments to all judicial proceedings.

IV. COLLECTION OF DIGITAL EVIDENCE AND CHALLENGES

It is important for investigator, before evidence gathering, to identify which documents or devices are to be collected. What type of evidence is required? Where is the evidence located? When the crime was committed? It means what period is required? Whose data is relevant? As in digital environment, many people are working in an office, therefore, it is

necessary for the investigator to specify and indicate the specific person from whose data is to be collected and lastly how the digital evidence will be collected?[41]

Digital evidence is fragile and it can "easily be manipulated, changed, modified, encrypted, and destroyed, making the job more difficult for the investigator to identify the relevant evidence."[42] In addition to this, digital "evidence is comprised of three main elements, the first being binary data, the second being a storage device on which to store that binary data and thirdly, software to read and interpret the binary data."[43] Furthermore, digital evidence may have been "altered, changed or modified by the criminals to remove all traces of its existence on computer."[44] Making more difficult for the investigator to trace "evidence of such modification may not always be possible to identify."[45] Although, criminal use sophisticated techniques to alter the digital information. Therefore, it is an established fact that "digital evidence may be modified without leaving any obvious trace of the commission of a transgression."[46] Therefore, expert witness requires certain level of expertise and he has to make considerable efforts to identify the modification of evidence.

Electronic crime is difficult to "investigate and prosecute, investigators have to build their case purely on any records left after the transactions have been completed."[47] In addition, electronic records are very malleable and electronic transactions currently have fewer limitations, which make it further difficult to investigate properly as computer records can be straightforwardly modified or destroyed. Additionally, computer transactions are very much fast, "they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible."[48]

Technological advancements pose various challenges while acquiring digital evidence which involves specialized skills, although, these are not required for physical evidence collection. Experts use various methods for extracting digital evidence from diverse variety of electronic devices. Still, these devices change rapidly. Therefore, investigators "need to either develop specific technical expertise or rely on experts to do the extraction for them."[49] Now this is an admitted fact that digital evidence in existing regime can easily be altered, manipulated, changed and destroyed creating new challenges for digital investigators. As digital evidence can be "altered or obliterated either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion."[50] Therefore, digital evidence creates many challenges for LEAs, lawyers, judiciary, digital forensic examiner and

[41] Allison Rebecca Stanfield, "The Authentication of Electronic Evidence," (Ph.D. diss., Queensland University of Technology, 2016), 124.

[42] Mahboob Usman, Dr. Muhammad Mushtaq Ahmad, "Admissibility of Circumstantial Evidence in Shariah and Pakistani Legal System," *Zia-e-Tahqeeq* 11 (2021): 13-23, 14.

[43] Stanfield, "The Authentication of Electronic Evidence," 4.

[44] Usman and Mushtaq, "Admissibility of Circumstantial Evidence," 14.

[45] Boddington, *Practical Digital Forensics*, 72.

[46] Ibid., 296.

[47] John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. (Massachusetts: Charles River Media, Inc., 2005), 218.

[48] Ibid., 219.

[49]https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018).

[50] Casey, *Digital Evidence and Computer Crime*, 26.

analysts. Digital evidence is circumstantial in nature,[51] therefore, it is difficult to attribute to some specific computer activity or to an individual. In some cases, the digital evidence is the sole evidence in any criminal or civil investigation. If a case is established on a single piece of digital evidence, then the case is "unacceptably weak" for prosecution point of view. Thus, without providing additional information, "it could be reasonably argued that someone else used the computer at the time."[52] Nowadays, it is common in institutions to use computer without entering the password as these computers are not password protected. So, at the time of prosecution, if the defense lawyer is successful in establishing that certain digital evidence was not obtained from the specific system, then this situation will weaken the case to award punishment relaying on this evidence alone.

More specifically, evidence dynamics create both investigative and legal challenges for digital forensic examiners and legal fraternity, making it further problematic "to determine what occurred and making it more difficult to prove that the evidence is authentic and reliable."[53] There are some special problems attached with computer data as computer data changes every moment which is invisible to human eye, process of data collection may change, and computer technologies are always changing.[54] Besides, digital evidence presents unique challenges which are not found in paper based evidence such as it is "easily modified, volatile, and easily duplicated and dispersed."[55]

Almost every device is now password protected and encryption software are being used to protect data from unauthorized users. Thus, both are the ultimate challenges faced by the investigators. Although, password protection is straightforward challenge as there are variety of tools "available for obtaining, circumventing, or guessing passwords on different file types."[56] Encryption protected data is very difficult to unlock as "encryption locks data with a key and only people with the appropriate key can unlock the data."[57] Whereas to de-encrypt the encrypted data specialized knowledge and equipment are required. There are many challenges associated to the computer evidence authenticity, which pose a serious challenge for the LEAs, judiciary, forensic expert and the investigators, making it very difficult to understand the exact nature and authenticity of the same. The following are the main challenges:

i. Whether the data was altered?
ii. Whether the program, which was used for generating the data, is reliable?
iii. Identity of the author?

The utmost care is exercised by the investigator to avoid the allegation of alteration of data or evidence, while collecting the data the investigator maintains proper chain of custody, document every action performed or taken to reply in case of question regarding the alteration of data, more specifically to counter the challenge of "was the data altered?" Reliability of

[51] Usman and Mushtaq, "Admissibility of Circumstantial Evidence," 15.
[52] Casey, *Digital Evidence and Computer Crime*, 26.
[53] Ibid., 28.
[54] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 19.
[55] John Sammons, *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*. 2nd ed. (Amsterdam: Elsevier, 2015), 114.
[56] Casey, *Digital Evidence and Computer Crime*, 458.
[57] Ibid.

programs is substantiated in the light of principles set out in the case of *Lorraine v. Markel American Insurance Company.*[58] However, author's identification is often countered with corroboration of circumstantial evidence. Regardless of complexity and detailed nature of computer forensics, instead of drawing the conclusions too quickly, "it is important for forensics investigators to focus on the facts of the collected data in their reports."[59]

There are some programs and processes which cause problems in digital investigation. According to Shavers these includes "peer-to-peer networking applications, open remote connections, active file deletion or file copying, and active program installations. Closing some programs, such as Internet Explorer, may cause user created data to be written to the drive, which may be beneficial to the examination."[60] When some applications are closed on a running system, then they may lose data.[61]

Law has prescribed procedure for everything presented in the court. Same is true for digital evidence which is "identified, collected, transported, stored, analyzed, interpreted, reconstructed, presented, and destroyed through a set of processes."[62] If the process performed during any stage from collection to presentation in the court, which is imperfect, this may cause a challenge. Although, there are valid legal challenges, that needs to be addressed by the presenter of evidence.

Multiply challenges, legal, technical and political are faced by LEAs which includes access to cross-border data, data retention, lacunas in legal system, an increasingly globalized online environment, lengthy and outdated procedures and practices, lack of proper education and training, lack of proper and up-to-date tools and resource to manage highly expensive investigation and if the evidence in is another country then outdated and lengthy mutual legal assistance practices. In view of emerging requirements of LEAs, legal issue may be addressed by providing legal cover to the issues faced by LEAs. In addition to legal solutions, "professionalisation in the field of digital forensics is necessary."[63] Therefore, proper education and training in imperative. The greatest challenge faced by the LEAs is cloud computing system. Where data is stored in cross-border servers, making more difficult for LEAs to trace and collect the data. Getting access on cloud system, recovering the required data, and processing for prosecution is very difficult. Even the US government, after getting search warrant from the competent court, was not able to get evidence from the Microsoft[64] until she enacted the "Clarifying Lawful Overseas Use of Data Act (CLOUD Act, 2018)."

[58] *Lorraine v. Markel American Insurance Company,* 241 F.R.D. 534 (D. Md. 2007)

[59] Christopher L.T. Brown. *Computer Evidence: Collection and Preservation,* 2nd ed. (Boston: Course Technology PTR, 2010), 21.

[60] Brett Shavers, *Placing the Suspect behind the Keyboard Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects* (New York: Elsevier, 2013), 15.

[61] Ibid.

[62] Thomas A. Johnson. *Forensic Computer Crime Investigation (*New York: CRC, 2005), 149.

[63] Biasiotti et al. *Handling and Exchanging Electronic Evidence across Europe*, 382.

[64] *Microsoft v. United States,* No. 14-2985 (2d Cir. 2016). US Department of Justice filled appeal to the US Supreme Court. While pendency of the case, US Congress passed the CLOUD Act, 2018, by amending the SCA to resolve controversy of jurisdiction related to the initial warrant.

V. EXPERT WITNESSES AND DIGITAL EVIDENCE

Boddington says "evidence is blind and cannot speak for itself, so it needs an interpreter to explain what it does or might mean and why it is important to the case, among other things."[65] The same rule is true for digital evidence where forensic expert interpret the evidence.[66] As per Black's law dictionary expert witness is defined as "[e]vidence about a scientific technical, or professional issue given by a person qualified to testify because of familiarity with the subject or special training in the field."[67] In Pakistani legal system, in various legal instrument, expert is defined such as in Article 59 of the QSO, the Investigation for Fair Trial Act, 2013,[68] section 510 of the CrPC and section 2 (f) of the Punjab Forensic Science Agency Act, 2007.[69] In section 510 of the CrPC, various experts have mentioned but forensic expert is not mentioned there.[70] Feeling this lacuna, the Government of Punjab has amended this section to include forensic expert. Section 40 of the PECA provides for establishment of forensic laboratory to provide for expert opinion in electronic evidence and similarly, section 46 of the said Act provides for seeking expert opinion.

The job of forensic expert is not an easy task, while examining digital data he has to "plow through thousands of active files and fragments of deleted files to find just one that makes a case. Computer forensics has been described as looking for one needle in a mountain of needles."[71] Digital evidence, cannot be provided in court by layman, in every case, where digital evidence is to be provided in the court, therefore, services of expert witness will be required to explain what he did to the computer and its data during examination of digital evidence. The investigating agency, producing digital evidence in the court, make ensure that the expert witness not only "has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination."[72] Further, the investigating agency must also ensure that her expert has up-to-date knowledge of his field and he has received training.[73] Likewise, forensic expert having training in law, will be more effective and will be in better way to give testimony in the court. Thus, while dealing with digital evidence, he will be in better position to handle the digital evidence in sound manners.

The expert opinion is not immune from challenges, this can be challenged upon any ground by any party privy to the judicial proceedings. The U.S.A Supreme Court settled the basic standard of expert testimony in *Daubert*[74] case. These standards were affirmed in *Kumho Tire v. Carmichael*.[75] *Daubert* principles[76] are being used by the courts in evaluating expert witness's testimony.

---

[65] Boddington, *Practical Digital Forensics*, 14.

[66] Mahboob Usman, Dr. Muhammad Mushtaq Ahmad, "Digital Evidence as a Shahada in Pakistani Laws and its application in the Courts," *Zia-e-Tahqeeq* 10 (2020): 37-49, 39.

[67] Black's Law Dictionary, 7th Edition, s.v. "expert evidence."

[68] Section 3(f) of the IFTA.

[69] Section 2(f) of the Punjab Forensic Science Agency Act, 2007 (Act No. XIII of 2007).

[70] Usman and Mushtaq, "Digital Evidence as a Shahada in Pakistani Laws," 39.

[71] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 59.

[72] Ibid., 9.

[73] Mason and Seng, *Electronic Evidence*, 23-24.

[74] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

[75] *Kumho Tire v. Carmichael*, 526 U.S. 137 (1999).

[76]

The first ever conviction in Pakistan was case of *Ahmad Omar Sheikh,*[77] where Anti-Terrorism Court convicted the accused persons, *inter alia,* on the basis of forensic expert report. However, this conviction was challenged in the Sindh High Court (SHC) and the SHC acquitted the accused persons[78] and the Supreme Court of Pakistan maintained the said decision.[79] The report of expert witness is admissible as held by the SHC in *Arif Hashwani v. Sadruddin Hashwani*[80] case but the accused cannot be convicted merely on the basis of expert opinion, rather other collaborative evidence is required as held by the SHC in *Abdul Ghani v. the State*[81] case where the court held that the report of expert is after all "an opinion which can be fallible and not immune from judicial scrutiny. The opinion of an expert is received in evidence because it either confirms or falsifies other evidence on record." Similar, view was taken by the SC in the *Land Acquisition Collector vs. Muhammad Sultan,*[82] where the court held that expert opinion is relevant and carries some probative value. However, in recent case of *Muhammad Idress v. the State,* the SC declared that the opinion of police officer is not relevant fact as he is not an expert.[83]

VI. TESTIMONY OF EXPERT WITNESS IN SHARI'AH

Expert opinion is one of the strongest testimony in Islamic Law, which help the presiding officer to determine a fact out of the issues. A witness can be qualified as an expert by acquiring required education, experience, skill, or training in the relevant field. Opinion of experts is given due importance in Shari'ah. Evidence of recognition of expert testimony can be driven from the verse of the Holy Qur'an. It is said in the Holy Qur'an:

"وَمَآ أَرۡسَلۡنَا مِن قَبۡلِكَ إِلَّا رِجَالٗا نُّوحِيٓ إِلَيۡهِمۡۚ فَسۡـَٔلُوٓاْ أَهۡلَ ٱلذِّكۡرِ إِن كُنتُمۡ لَا تَعۡلَمُونَ[84]"

"We did not send (Messengers) before you other than men whom We inspired with revelation. So, ask the people (having the knowledge) of the Reminder (the earlier Scriptures), if you do not know."[85] While commenting on this verse of Holy Qur'an, Abdullah Yusuf Ali, says "…may also mean any men of Wisdom, who were qualified to have an opinion in such matters."[86]

i. Whether the theory or technique can be (and has been) tested.
ii. Whether the theory or technique has been subject to peer review and publication.
iii. The known or potential rate of error of the technique or theory used.
iv. The existence and maintenance of standards and controls
v. Whether the technique or theory has been generally accepted in the scientific community.

[77] FIR no. 24/2002 dated 04.02.2002 registered at Police Station Artillery Maidan, Karachi (South) under various sections of PPC and ATA.

[78] *Ahmed Omar Sheikh v. the State*, 2021 YLR 1777.

[79] *The State v. Ahmad Omar Sheikh*, 2021 SCMR 873.

[80] *Arif Hashwani v. Sadruddin Hashwani,* PLD 2007 Karachi, 448.

[81] *Abdul Ghani v. State,* 2007 YLR 969.

[82] *Land Acquisition Collector v. Muhammad Sultan,* PLD 2014 Supreme Court 696.

[83] *Muhammad Idress v. the State,* 2021 SCMR 612.

[84] Qur'an 16: 43.

[85] Translation of this verse has been taken from Quran-e-Karim by Mufti Taqi Usmani.

[86] The Holy Qur'an: Text, Translation and Commentary, by Abdullah Yusuf Ali.

There are number of *ahadith* of the Prophet Muhammad (ﷺ) which recognize evidence of expert witness. It has been related on the authority of Ayesha (R.A) who said that one day the Prophet Muhammad (ﷺ) came to her and said with exciting mood, "Oh Ayesha, don't you see that *Mujazzaz Al-Mudlaji* came and saw that *Zaid* and *Usamah*, lying being covered with a sheet in a position that their heads were covered but their legs were uncovered, and said, these legs are from one another.[87] *Mujazzaz Al-Mudlaji* was an expert on lineages. Companies of Holy Prophet (ﷺ) also relied upon evidence of experts.

In the era of Hazrat Umar (R.A), a woman and young man from Ansar were brought to Hazrat Umar (R.A). In fact, the woman loved the young man but he did not like her. Therefore, she planned a tactics and broke an egg on her clothes and thighs. Thereafter, she blamed the young man for attempting sexual intercourse and produced clothes as a proof. Hazrat Umar (R.A) asked a woman to examine the evidence. The woman affirmed that there is semen on her clothes and thighs. When Hazart Umar (R.A) decided to punish the man, he stood up and said, O *Amir al-Mu'ammin*, I have not committed any offence, rather the woman planned to deceive you. Thus, Hazrat Umar (R.A) asked Hazrat Ali (R.A) to bring water and Umar threw the water on her clothes and thighs. By testing this he knew that it is an-egg and she confessed her mistake.[88]

Similarly, a black man complained to Hazrat Umar (R.A) by saying that I am black, and my wife is also black. But despite this fact my wife has given birth to a red child. However, the wife rejected this allegation and informed Hazrat Umar (R.A) that this is our legitimate child and I have not committed illicit sexual intercourse with anybody. Then, Hazrat Umar (R.A) asked Hazat Ali (R.A) about the situation, Hazarat Ali (R.A) inquired from the man, have you met your wife during her periods? He said, Yes, Hazarat Ali (R.A) held when human sperm mixes with blood, it gives birth to a red child.[89] On the basis of opinion of Hazarat Ali (R.A) this issue was decided. Thus, it can be safely said that the expert testimony was also being used during the era of Holy Prophet (ﷺ) and his Companions.

VII. Conclusion

Dealing with digital evidence is a challenging task, starting from its creation to production in proceeding before the courts, all these stages require special expertise and training to handle it. At every stage, there are legal as well as technical issues attached to it. This evidence is produced through expert witness, there are many legal instruments which discuss the experts, but the forensic expert is not discussed in section 510 of the CrPC, therefore, there is a dire need to amend the said section to make the report of forensic expert admissible, following the footsteps of the Government of Punjab in this regard while amendment in the province of Punjab has play a vital role in making a credible use of digital evidence in judicial proceedings. Besides, as per section 29 of the ETO, all amended brought in the QSO through ETO are only meant for ETO and are not extended to other laws, instead of realizing this aspect, the courts, incorrectly, applied the same amendment in every case

[87] *Sahih al-Bukhari*, 6770*; Sahih al-Bukhari*, 3555*; Sahih Muslim* 1459*; Sunan Abi Dawud*, 2267; *Jami` at-Tirmidhi*, 2129.

[88] Muhammad Ibn Abu Bakr Shams al-Din Ibn al-Qayyim Al-Jawziyyah, *Al-Turuq Al-Hukmiyyah fi Siyasah al-Shar'iyah* (Cairo: Maktaba al-Muhammadiyah, 1973), 98.

[89] Ibn al-Qayyim, *Al-Turuq Al-Hukmiyyah*, 43

where some type of digital evidence was recovered. Thus, section 29 of the ETO be amended to apply amendments to all judicial proceedings.