DIGITAL EVIDENCE AS A SHAHADA IN PAKISTANI LAWS AND ITS APPLICATION IN THE COURTS

Mahboob Usman*, Dr. Muhammad Mushtaq Ahmad**

Abstract:
Because of globalization, world is moving fast and keeping pace with the Information technology is difficult for the countries, however, this makes more difficult for developing countries to handle this situation. As for the law-makers it cannot be expected to predict for the future, therefore, legislation designed for a specific objective may fail when a new situation arises. The same situation is faced by the legal fraternity, executive, legislature and judiciary alike in Pakistan, while dealing with digital evidence when the entire previous instrument on the law of evidence does not cover many aspects of the digital evidence. This article analyze, in the light of Shari'ah that how digital evidence is seen by the Courts in Pakistan. Digital evidence is brought through expert witness, thus the role of expert witness is also examined. At the end, assessment of digital evidence by the judges is discussed and lastly online courts and recording of evidence through video conferencing is deliberated.

Keywords: digital evidence, expert evidence, Sharia Laws, Qanun-e Shahadah

Introduction

Long before the use of information technology in courts, the only recognized medium was direct evidence recorded in the presence of the parties and the documents were exhibited in physical form. Nevertheless, technology has presented numerous challenges in evidence production in courts. Wacks has described it in the following words:

The emergence of information technology, to select only one obvious instance, poses enormous challenges to the law. Attempts legally to control the Internet, its operation or content, have been notoriously unsuccessful. Indeed, its very anarchy and resistance to regulation is, in the minds of many, its strength and attraction. But is cyberspace beyond regulation?[1]

The use of digital evidence "in courts can effectively be considered a major innovation in sphere of justice. Infact, as the justice system becomes increasingly digitized, many see the use of electronic evidence as a means of simplification, facilitation, acceleration, and rationalization, depending

* Mahboob Usman, PhD scholar at the Department of Law, Faculty of Shari'ah and Law, International Islamic University, Islamabad (IIUI) and can be reached through mehboob_usman@yahoo.com

** Dr. Muhammad Mushtaq Ahmad, Director General Shari'ah Academy, IIUI and can be reached through mushtaqahmad@iiu.edu.pk

on the circumstances."[2] The use of IT in courts provides inexpensive and expeditious justice to citizens as envisaged in the Constitution of Pakistan.[3] As the digital evidence can be manipulated easily, therefore, investigator's prime responsibility is to ensure that the digital "evidence was not altered between its acquisition and its presentation in legal proceedings and even before its acquisition by the practitioner."[4] Likewise, chain of custody of the exhibit "must be fully documented to account for its location and custodianship between seizure and presentation."[5] Investigator should also establish that the evidence was "protected from physical damage while being transported from the crime scene to the place of safekeeping and laboratories."[6]

Digital data is not like other type of data, as digital data "is not directly observable by the finder of fact, it must be presented through expert witnesses using tools to reveal its existence, content, and meaning to the fact finders." Digital evidence is hearsay evidence which is presented "by an expert who asserts facts or conclusions based on what the computer recorded, not what they themselves have directly observed." Expert witness plays an important role in digital evidence. Therefore, "it depends on the quality and unbiased opinion of the experts for each side."[7]

Need For Understanding of Technology

Law is integral part of society and the same cannot be separated from other fields. For instance, demand for understanding the link between law and technology is increasing. Whereas, forensic evidence "lies at the juncture between science, technology, and the law. In the age of information, everyone who plays a role in the justice system must be accountable to increased learning and knowledge in and around their domain."[8] Therefore, it is imperative for the legal fraternity "to understand the role of the expert witness, the attorney, the judge and the admission of forensic science evidence in litigation in our criminal justice system."[9] Handling of digital requires "sufficient knowledge of technical aspects to have an understanding of how to preserve evidence and how to evaluate and interpret the materials presented."[10] This also requires having "a basic knowledge of the technicalities of, software used in the discovery process, but also an understanding of social media, the technical options, and the way people use these media."[11] The existing judicial system, in Pakistan, is full of judges and lawyers "who generally lack the scientific expertise necessary to comprehend and evaluate forensic evidence in an informed manner."[12] Nevertheless, the assessment of digital evidence is more complex than other type of evidence.

Therefore, to assist the courts involving experts and "a proper understanding of their findings by courts and lawyers, the digitisation of society and proceedings requires tech-savvy judges and lawyers."[13]

Expert Witnesses

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."[14] The same is true for digital evidence where expert witness is required to interpret the evidence. In digital evidence, computer forensics expert has various responsibilities including identification, collection, preservation, examination, analysis, transportation and presentation of the digital data before the courts. Though, nothing is easy in digital evidence from identification to presentation in court. Therefore, investigators "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."[15] In every case, services expert will be required to explain what he did to the computer and its data during examination of digital evidence. Therefore, the investigating agency make ensure that expert not only "has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination."[16] Further, it is also important for an expert to have "up-to-date knowledge and receives constant training, which are more important than experience in this field."[17] Furthermore, he should also be "knowledgeable in the law, particularly legal jurisdictions, court requirements, and the laws on admissible evidence and production."[18]

However, generally expert witnesses' opinion is challenged by the opposing lawyer. The court should be sensitive in respect of expert testimony relating to digital evidence. Therefore, at least, the court should observe the Daubert[19] standards which were prescribed by the U.S.A Supreme Court. As such, the Daubert standard is applied by the courts to expert witnesses and the court in Kumho Tire v. Carmichael,[20] extended the Daubert standard to experts with technical or specialized knowledge. Daubert factors[21] are to be used by the courts in appraising expert witness's testimony, however, these factors are not limited and it may be possible that in certain circumstance some of these factors or all of them may not apply in a specific situation, but their significance cannot be ignored. Article 59 of the Qanun-e-Shahadat Order, 1984, section 2 (f) of the Punjab Forensic Science Agency Act, 2007,[22] the

Investigation for Fair Trial Act, 2013[23] and section 510 of the Code of Criminal Procedure, 1898 (CrPC) define and discuss the expert witness. However, section 510 of the CrPC discuss the reports of experts but forensic expert is not mentioned there. Punjab Government has amended the section 510 include the forensic expert. Sections40 and 46 of the Prevention of Electronic Crimes Act, 2016, discuss the expert opinions.

Sindh High Court (SHC) in Abdul Ghani vs. the State,[24] case 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." SHC in Arif Hashwani v. Sadruddin Hashwani,[25] held that expert evidence is admissible in evidence. In the Land Acquisition Collector vs. Muhammad Sultan,[26] the SC held expert opinion is relevant and carries some probative value. In Ahmad Omar Sheikh v. the State,[27] the trial court convicted the appellants, inter alia, on the basis of expert report regarding IP address, emails and laptop recovery. However, the SHC on the basis of contradiction in evidence acquitted the appellants.

Digital Evidence in the Courts

The basic purpose of any courtis to administer justice between the parties and the role of investigators is to investigate the matter and present evidences in the courts. Hence, courts are depending on the credibility and reliability of the evidence presented by the investigators, especially in cyber-crime cases where the courts heavily rely on the "digital investigators and their ability to present technical evidence accurately; it is their duty to present findings in a clear, factual, and objective manner."[28] Besides, courts are more "concerned with the authenticity of the digital evidence they present."[29] The evidence presented by the experts must meet the criteria set out by the in Daubertcase.

There are certain requirements for admission of evidence. For example, court will ensure that every evidence which is presented before him "is relevant and will evaluate it to determine if that is what its proponent claims, if the evidence is hearsay, if it is unduly prejudicial, and if the original is required or a copy is sufficient."[30] In case of failure to consider these issues, the evidence will not be acceptable. LEAs aim must be "to further strengthen their communication channels with those in the justice system, as this can contribute to enhancing the understanding of digital evidence within the judiciary, thereby potentially also alleviating LEAs from unnecessarily burdensome analysis requests."[31] Courts are

"struggling to determine how to address the myriad of evidentiary issues that arise when digital images and other computer generated information is presented in court."[32] Moreover, it has also created "unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures." Establishing admissibility through conventional method is well-settled now. However, "their applicability to digital data and devices from which electronic evidence is generated raise complex issues and questions."[33] Digital evidence in courts is presented through experts.

Neither the judges are much unfamiliar with technology, nor do the lawyers assist the courts properly resulting in challenging the integrity of evidence. Nonetheless, issues arising out of information technology are required to be adjudicated properly by the judiciary for accepting of evidence. Therefore, deliberate of the judiciary on the authenticity and trustworthiness of computerized data is vital. Voluminous digital data is another challenge, thus, verification of all items may not be possible. Hence, Judges must possess "a strong basic knowledge of computers, the Internet and cyber forensics. They must make decisions regarding probable cause in the issuance of search warrants and in preliminary hearings, the admissibility of cyber evidence, the appropriateness of expert testimony and many other significant legal issues."[34] This issue can be addressed by designation of special judges for the purpose.

While amending the QSO, it was specifically stated that these amendments shall apply to the extent of ETO but without reading of ETO, the provisions of ETO have been applied to every situation which is against the spirit of enactment. Therefore, it can safely concluded that this modification to the QSO is just for the ETO and thus not applicable to any other proceedings. This aspect has been ignored by the legal community. Then question arises why these amended were incorporated in QSO and applied to all law? This issue has not been discussed or addressed anywhere in Pakistani legal system. The reason appears that actually section 29 of the ETO was ignored and applied to other laws, which need to be rectified or the ETO should be amended.

How Courts assess the evidence

Judges developed countries have little knowledge about the latest technology. The same is true for developing countries. Due to lack of proper knowledge of digital evidence, judges accept it without questioning it credibility and authenticity. None of the Pakistani cases

digital evidence has been discussed properly. In Ishtiaq Ahmad Mirza v. Federation of Pakistan,[35] Supreme Court has provided some guidelines about its acceptance. Everywhere courts have recognized "that with the pervasiveness and increasing significance of digital evidence, there is a concomitant increase of risk of evidence being tampered with. Many courts recognize that digital evidence presents more complicated variations of the authentication problem than do paper documents."[36] Courts are required "to satisfy themselves as to the reliability of the evidence and the integrity of the forensic processes and tools used to procure, secure, and analyze the evidence throughout the entire forensic process."[37] In Lorraine v. Markel, the Judge Grimm observed that "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[38]

In court proceedings, while discussing "the admission of evidence from devices controlled by software code, judges do not distinguish between a single, highly specialist device that is self-contained, and a linked network containing any number of devices each independently operating on its own set of software code."[39] Therefore, it is imperative for judiciary to consider complications attached to it. How far computer expert's evidence meet the criteria prescribed by the QSO? In 80s, limited people were familiar with IT. Thus, it cannot safely be said that the drafter of the QSO were aware of modern day digital devices. Meaning thereby that existing digital devices are not covered under the Article 164 of QSO. In Kh. Ijaz Ahmad v. D.R.O, the Lahore High Court (LHC) held that neither the person who produced the video had recorded the video nor any affidavit of the person was produced, therefore, the video/film was not a legal piece of evidence and not accepted in evidence. In Ali Naqi v. Government of the Punjab,[40] the termination of services of the accused was upheld on the basis of making of video of female patient in the operation theatre. In Muhammad Nasir v. Mahmood Shaukat Bhatti[41] case the LHC held that "computer technically is a modern technique and is well within the ambit of" Article 164 of the QSO. Same view is affirmed by the Election Tribunal Balochistan in Muhammad Akram Baloch v. Akbar Askani.[42] In Umair Ashraf v. The State,[43] the SHC allowed the production of C.D in a criminal proceeding. In Rehmat Shah Afridi v. The State,[44] it was held that the tape recorded conversion is real evidence and can be accepted in the court proceedings. In Sikandar Ali Lashari v. the State,[45] the court allowed to provide USB and CD to the accused.

Nowadays, CCTV cameras are installed everywhere and same is used by the investigating agency to prove a fact. Mason has discussed about CCTV cameras in the following words:

Surveillance cameras are very much part of life in the twenty-first century, ever since the foundations of their use were laid in the latter decades of the twentieth century. Evidence of images from security cameras can be very helpful in identifying the perpetrators of crimes. Such evidence has been admitted in English courts, mainly in criminal cases.[46]

The SHC in Ammar Yasir Ali v. The State,[47] has provided the criteria for acceptance of CCTV footage in evidence and the SC in Asfandyar v. Kamran,[48] held that:-

Mere producing any footage of C.C.T.V. as a piece of evidence in the Court is not sufficient to be relied upon unless and until the same is proved to be genuine. In order to prove the genuineness of such footage it is incumbent upon the defence or prosecution to examine the person who prepared such footage from the C.C.T.V system.

In Government of Sindh v. Fahad Naseem[49] the SHC directed the prosecution agency to provide video cassette to the defendants as the video cassette is accepted in evidence. Similarly, in Nazim Ali vs. Additional Sessions Judge,[50] the LHC directed the prosecution agency to provide memory card to the accused. The LHC in Hashim Jamal v. the State,[51] refused bail of the accused on the basis of forensic evidence collected from cell phone handset. In Junaid Arshad v. the State,[52] the court also refused bail on the basis of evidence collected from cell phone and IP address. In Zakir Hussain v. The State,[53] the Chief Court of Gilgilt-Baltistan, upheld the conviction of the accused on the basis of confection recorded on CD. In Muhammad Jawad Hamid v. Muhammad Nawaz Sharif,[54] the LHC held that video recording statements of accused had to be proved by its author and creator. In Shahid Zafar v. the State,[55] the court accepted the DVD cassette/video recording, produced in trial court as admissible evidence. In Muhammad Irfan v. The State,[56] the LHC accepted the evidence on mobile phone memory card and upheld the conviction of the accused and the SC has taken an exhaustive survey of jurisprudence on the subject of digital evidence in the case of Ishtiaq Ahmed Mirza v. Federation of Pakistan[57] and authoritatively settled parameters to receive forensic evidence through modern devices and techniques. In evidence relying upon on video recording, it is necessary to prove before court that the video is genuine, if the video is examined by

the forensic analyst, the forensic analyst's report is admissible. However, for relying upon such report, its court's discretion to accept the same, if accepted that needs to be proved in accordance with settled law of Pakistan. Thereafter, source video becoming available along with the date of acquiring of the video tape is to be disclosed by the person producing the video. The person desiring to produce the video tape has to make an application before the court for bringing on the record, however, if the video tape is produced at a later stage, then the same may be looked with suspicion.

To prove the accuracy of the video recording other evidence must be provided to rule out any possibility of tampering with the video. Besides, the video must be actual recording of the conversation of any event and the person recording the video has to be produced before the court to produce there cording himself in the court which same must be played before the court and person recording the conversation must identity the voice of the person speaking or the person seen in the video, however, the video produced before the court should be clearly audible or viewable. Besides, any other person present at the time of making video may also testify about the event. Moreover, the person shown in the video must be properly identified. The evidence produced through video recording must be admissible and relevant to the controversy. Proper chain custody of evidence must be proved. If the transcript of video is prepared then the same must be prepared under the independent supervision and control. In Ishtiaq Ahmed Mirza v. Federation of Pakistan[58]case the SC held:

The person recording an audio tape or video may be a person whose part of routine duties is recording of an audio tape or video and he should not be a person who has recorded the audio tape or video for the purpose of laying a trap to procure evidence.

Digital information on digital devices have very important aspects of digital data which have not been examined so far. Some questions can be raised about the digital evidence.

Who created/recorded/copied the video?

What is the date, time and place of recording of the video?

Whether the videoremained in safe custody?

Whether proper chain of custody is maintained?

In case of CCTV, character of the person who operate the system?

Whether the metadata is intact? If so, whether the same is original or altered?

What devices were used to create the video?

What is the security control procedure?

If video is posted on social networking website, who posted them? What is the source of video?

Who can testify about accuracy of the video? What will be the procedure of authentication?

Whether any analysisby the forensic expert was done?

Whether the law will accept it primary or secondary evidence?

Whether the video was encrypted or not?

In Umair Ashraf v. the State,[59] the SHC, held that "evidence which has been collected by the prosecution by way of modern device cannot be disallowed," and the SHC allowed to play the CD. In Muhammad Sadiq v. the State,[60] the LHC held that "Under the law evidence collected through modern devices is admissible in evidence and the same can be used against the accused during judicial proceedings to determine the questions of criminal liability or as the case may be." Therefore, the LHC on the basis of confession recorded by the police on CD upheld the conviction of the accused.

The concept of E-Courts in Pakistan

In May 2019, SC started the hearing of appeal through video conferencing. After getting fully equipped with latest digital device courts will be able to proceed with online trial, this will save time and resources making ease for litigations to get speedy justice. In electronic trial documents are "available electronically via online systems, directly to the court, and where the documents themselves can be displayed electronically to those in the courtroom."[61] There are many benefits of electronic trials which are not available in manual trials such as "they can save an inordinate amount of time as the lawyers involved in the hearing do not have to spend time finding each individual page being referred during the hearing, as the document is available on screen within seconds of counsel referring to the document identifier."[62] Besides, benefits of electronic trials in small and complex matters are same, such as "they result in the display of documents much more quickly, allowing those present in the courtroom to view the documents quickly and easily, without the need for each party to go to cumbersome hard copies and wait for everyone else to be on the same page."[63] Hence, short time is consumed by the courts as compared to conventional system. Whatever the matter is, the end result will be "the more efficient use of technology to enable documents to be accessed quickly and easily, with cost savings to the

litigant."[64] All types of court proceedings can be conducted electronically. Online hearing, if continued successfully, will benefit the legal fraternity as well as litigants by making judicial system more responsive to the needs of Pakistani people in redressing their grievances, and will save the precious time and reduce the burden of litigants.

Recording of evidence through video conferencing

In conventional evidence recording witness are present in courts while in online court proceedings witness are not present in court room. Video conferencing "will be available for those witnesses who are unable to travel long distances and are able to appear remotely, and the use of streaming video across the internet means cost effective video is much more accessible."[65] In Watan Party v. Federation of Pakistan[66] SC appointed a commission for evidence recording through video conferencing. The SHC in Aijazur Rehman v. the State,[67] has stressed upon the use of modern technologies for speedy trial. In Muhammad Nawaz Sharif v. the State,[68] IHC upheld the decision of trial court for recording of evidence through video link.

Punjab government has amended[69] the Family Court Act, 1964 to provide for recording of evidence through video recording in family matters. In the case of Salman Ahmad Khan v. Judge Family Court[70] the LHC upheld the decision of family court in which it was directed to record evidence through skype. In serious offences, "the court may examine a witness through video link."[71] In Muhammad Arif Chaudhry v. Muhammad Suleman[72] the SC proposed the hearing of cases through video conferencing. This is effect mechanism for adjudication of cases in any emergency situation. Therefore, it can safely be concluded that recording evidence through video conferencing is blessing which can be utilized to save resource and expedite the process of conclusion of trial.

Conclusion

The presentation of evidence is last stage in investigation. In digital evidence instead of presenting original object, the print out or the expert report is presented in court proceedings. Thus, it is necessary that the expert must be having education, skill and training in digital forensic. Besides, judges, lawyers and prosecution should also be having some basic understanding of digital forensic to examine, scrutinize and present digital evidence in proper admissible way. Failing to understand digital forensic by the professionals may lead to wrong conviction or acquittal of the accused. Moreover, the criminal procedure code does not include

forensic expert in the category of expert which need to be amended to include the forensic expert and remove the lacuna. By adopting latest techniques and technologies in court proceeding, the inexpensive and speedy justice can be provided to Pakistani people as envisaged in the Constitution of 1973.The world is moving too fast and have adopted various technique to expedite the trial process. Hence, have adopted video conferencing method for trial as well as for appeal. Although, the SC has adopted this method for appeal, which is not sufficient. This should be extend to all the High Courts and same should also be used for trial purposes, which will save time and resources of the government as well as litigants.

References

1. Raymond Wacks,*Law A Very Short Introduction* (Oxford: Oxford University Press, 2008), 133.
2. Maria Angela Biasiotti et al. *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 289.
3. Article 37 (d) of the Constitution of the Islamic Republic of Pakistan, 1973.
4. Richard Boddington, *Practical Digital Forensics* (Birmingham: Packt Publishing, 2016), 93.
5. Ibid., 94
6. Ibid.
7. Thomas A. Johnson. *Forensic Computer Crime Investigation* (New York: CRC, 2005), 150-51.
8. Amy Lynnette, "Digital and Multimedia Forensics Justified: An Appraisal on Professional Policy and Legislation," (M.S. diss., University of Colorado Denver, 2015), 27.
9. Amy Lynnette, "Digital and Multimedia Forensics Justified," 27.
10. Xandra Kramer, "Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise," *JornadasIberoamericanas de Derecho Procesal*, XXVI (2018): 391-410 at 409.
11. Kramer, "Challenges of Electronic Taking of Evidence," 409.
12. Amy Lynnette, "Digital and Multimedia Forensics Justified," 29.
13. Kramer, "Challenges of Electronic Taking of Evidence," 410.
14. Boddington, *Practical Digital Forensics*, 14.
15. John R Vacca. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. (Massachusetts: Charles River Media, Inc., 2005), 59.
16. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 9.
17. Mason and Seng, *Electronic Evidence*, 23-24.
18. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 155.
19. *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
20. *Kumho Tire v. Carmichael,* 526 U.S. 137 (1999).
21
    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.

22. Section 2(f) of the Punjab Forensic Science Agency Act, 2007 (Act No. XIII of 2007).
23. Section 3(f) of the IFTA.
24. *Abdul Ghani v. State,* 2007 YLR 969.
25. *Arif Hashwani v. Sadruddin Hashwani,* PLD 2007 Karachi, 448.
26. *Land Acquisition Collector v. Muhammad Sultan,* PLD 2014 Supreme Court 696.
27. *Ahmad Omar Sheikh v. State*, Appeal no. 66-68/2002 in SHC decided on 02.04.2020.
28. Eoghan Casey, *Digital Evidence and Computer Crime, 3rd ed.*(New York:Elsevier, 2011), 49.
29. Casey, *Digital Evidence and Computer Crime,* 49.
30. Ibid.
31. Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 382.
32. https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).
33. Ibid.
34. Marcella and Menendez, *Cyber Forensics*, 308.
35. *Ishtiaq Ahmad Mirza v. Federation of Pakistan*, 2019 PLD SC 675.
36. Boddington, *Practical Digital Forensics,* 86.
37. Ibid., 91.
38. *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D. Md. 2007).
39. Mason and Seng, *Electronic Evidence*, 113.
40. *Ali Naqi v. Government of the Punjab,* 2019 PLC (C.S.) 952 Lahore.
41. *Muhammad Nasir v. Mahmood Shaukat Bhatti,* PLD 2003 Lahore 231.
42. *Muhammad Akram Baloch v. Akbar Askani,* 2014 CLC 878.
43. *Umair Ashraf v. The State,* 2008 MLD 1442.
44. *Rehmat Shah Afridi v. The State*, PLD 2004 Lahore 829.
45. *Sikandar Ali Lashari v. the State,* 2016 YLR 62 (Sindh).
46. Mason and Seng, *Electronic Evidence*, 61.
47. *Ammar Yasir Ali v. The State,* 2013 PCRLJ 783. In *Babar Ahmad v. The State*, 2017 YLR 153, the Gilgit-Baltistan Chief Court, accepted CCTV footage in evidence.
48. *Asfandyar v. Kamran*, 2016 SCMR 2084.
49. *Government of Sindh v. Fahad Naseem,* 2002 PCRLJ 1765 Karachi.
50. *Nazim Ali v. Additional Sessions Judge,* 2016 MLD 25.
51. *Hashim Jamal v. the State,* 2018 YLR Note 105.
52. *Junaid Arshad v. the State,* 2018 PCrLJ 739 (Lahore).

53. *Zakir Hussain v. The State*, 2017 PCrLJ 757. The same view was taken by the LHC in *Muhammad Sadiq v. State,* 2016 PCrLJ 1390, in which the LHC held that evidence recorded on CD is admissible in criminal cases.
54. *Muhammad Jawad Hamid v. Muhammad Nawaz Sharif,* 2019 PCrLJ 665 (Lahore).
55. *Shahid Zafar v. the State,* 2015 PCrLJ 628 (Sindh).
56. *Muhammad Irfan v. The State*, 2018 PCRLJ 1319.
57. *Ishtiaq Ahmed Mirza v. Federation of Pakistan,* PLD 2019 SC 675.
58. *Ishtiaq Ahmed Mirza v. Federation of Pakistan,* PLD 2019 SC 675.
59. *Umair Ashraf v. The State,* 2008 MLD 1442 (Karachi).
60. *Muhammad Sadiq v. the State,* 2016 PCRLJ 1390.
61. Allison Rebecca Stanfield, "The Authentication of Electronic Evidence," (Ph.D. diss., Queensland University of Technology, 2016), 181.
62. Ibid.
63. Ibid., 183.
64. Ibid., 184.
65. Ibid.
66. *Watan Party v. Federation of Pakistan,* PLD 2012 SC 292.
67. *AijazurRehman v. the State*, PLD 2006 Karachi 629.
68. *Muhammad Nawaz Sharif v. the State,* PLD 2018 Islamabad 148.
69. Section 11 (1A) of the Family Courts Act, 1964 (Act XXV of 1964).
70. *Salman Ahmad Khan v. Judge Family Court,* PLD 2017 Lahore 698.
71. Section 10 of the Punjab Witness Protection Act, 2018 (Act XXI of 2018).
72. *Muhammad Arif Chaudhry v. Muhammad Suleman*, Civil Petition No. 1945/2018, order dated 16.04.2020.