Pakistan Social Sciences Review
www.pssr.org.pk

RESEARCH PAPER

Admissibility of Digital Evidence: A perspective of Pakistani Justice System

Dr. Usman Hameed [1] Zarfishan Qaiser [2] Khushbakht Qaiser *[3]

1. Director School of Law and Policy, University of Management and Technology, Lahore, Punjab, Pakistan
2. Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan
3. Assistant Professor, School of Law and Policy, University of Management and Technology, Lahore, Punjab, Pakistan

PAPER INFO

Received:
July 21, 2021
Accepted:
November 26, 2021
Online:
November 29, 2021

Keywords:
Admissibility,
Authenticity
Digital Evidence,
Reliability

***Corresponding Author**
Khushbakht.qaiser@umt.edu.pk

ABSTRACT

Digital evidence is any evidence which can be stored, exchanged or generated in electronic form. Such type of evidence has assumed a crucial role in modern day adjudication of criminal cases. In the recent past, digital evidence was treated as secondary evidence in Pakistan, however, keeping in view its increasing relevance to detect and punish crimes in the information age, some critical legislative changes were made to give the status of primary evidence to the digital evidence. This article suggests that the status of digital evidence has become primary to the extent of its admissibility only. In relation to weight or appraisal, it is still regarded as a circumstantial evidence requiring corroboration. This approach can be changed by judicial precedents implementing the changes brought about by the legislature.

Introduction

With a view to arrest the growth of rising digital criminality and addressing concerns about the admissibility of digital evidence to prove such crimes, the legislature of Pakistan enacted Electronic Transactions ordinance 2002 (ETO). The ordinance brought some fundamental changes to the traditional law of evidence applicable to civil and criminal trials. Basically, what the ordinance did was to declare the electronic or digital evidence as primary. It also affirmed the originality of electronic documents, information, record and transaction and thereby dispelling the perception that the information stored or exchanged digitally is hearsay evidence. Secondly, the ordinance underscored the fact that digital evidence qualifies the Best evidence standard. Likewise, the ETO 2002 reaffirm the relevance of digital evidence

apparently keeping in view the dictates of Article 18 QSO 1984 according to which evidence may only be led as to matter in issue or relevant facts

This article suggests that while the promulgation ETO 2002 is commendable in the sense that it has clarified the status of digital evidence and at the same time diminished the total reliance of the courts on article 164 QSO which tends to be a permissive rather than obligatory provision and leaves much to be desired in terms of explaining what is a modern device. However, in view of some observations of the judges of the superior courts of Pakistan, it appears that the evidence has been declared primary and capable of qualifying best evidence test to the extent of its admissibility, its appreciation or weight is still left to the discretion of the court. Therefore, in terms of weight it may not be wrong to suggest that digital evidence is still corroboratory evidence. When we speak of primary evidence, there is a difference between computer stored and computer-generated evidence. As ETO 2002 only regards that evidence primary which is original and unaltered barring natural additions or decay, the computer-generated evidence appears to qualify the test of originality such as transaction receipts because no further copies can be made after the first one. On the other hand, the computer stored evidence has to be taken with a pinch of salt because it can be altered or added to. In other words, it can be treated corroboratory. The article will suggest that in order to appreciate as opposed to admit electronic evidence, it must be weighed against the time-tested factors as outlined in the international best practices such as authenticity, reliability, chain of custody and reliability.

Uses of Digital Evidence in 21st Century

In modern times use of digital devices has recorded exponential increase in doing all kind of activities. For example, all correspondence is done through email or instant messages. Likewise, digital images have taken the place of traditional photography. Digital documents are used to spell out terms of the contract and the acceptance of the contract is also done digitally. However, digital activities and in person ordinary activities have a fundamental difference. All the steps taken in a digital activity can be traced, in other words digital activity leaves a record which can be traced. To illustrate, even if you delete something in your computer files, it can be retrieved. While the action of delete will leave space on the storage device whether it's a hard disk, USB or floppy disk, it can be discovered either from on line storage engines such as cloud or through the network administrator. In short, every step that a person takes on a digital device can be traced back. On the other hand, when something is done physically, it is possible to eliminate every evidence of your crime. Because of this, digital evidence has tremendously grown in importance since the beginning of 21st century. This brings us to the point where we need to define the digital evidence.

Explanation of the Concept of Digital Evidence

Any information stored or exchanged in a digital form and meant to be used as a proof in a court of law is called digital evidence. The term digital means that the information is in binary form of 0s and 1s and cannot be understood with naked eye.

Is it secondary evidence?

In order to decipher this information, some other process is required to be applied. For example, a printer will be required to get a print out in readable for. However, in view of the application of a second process it is sometimes said that the information derived from a digital storage device such as hard disk, floppy disk or USB is secondary evidence. This view of regarding digital evidence as secondary evidence stood ground for a long time. Nonetheless, when technology became affordable and GPS tracking devices and mobile phones reached every nook and canny of the world, it was realized that information stored in digital devices and exchanged over two computer networks could be of great use in regard to tracing crimes and movements of the offender. For example, CCTV footage, audio and video recordings, instant messages and digital images all can be used to prove the crime and to trace the offender. Consequently, many justice systems of the world brought changes to their rules of evidence and brought digital evidence at par with traditional oral or documentary evidence.

Digital Evidence can be modified or altered

In any case, if digital evidence has the quality of not being easily deleted or removed it also has a weakness that digital evidence can be easily modified, altered or destroyed. Therefore, in order to ensure the reliability and authenticity of digital evidence certain measures are required to be taken. For example, first responders to a crime scene with digital evidence must be experts of digital forensics. Forensics means application of science to legal situations or legal question. So, if the layman tries to store or extract digital evidence, there is an apprehension of important evidence getting lost, destroyed or altered. To illustrate, damage can be caused to the disk while extracting evidence. Secondly, it is of utmost importance that all processes applied to digital evidence must be recorded to preserve its authenticity. In other words, a log must be maintained describing when and how it was extracted, by whom and to who it was handed over. This important aspect will be discussed later in the article to suggest what steps are required to be taken to prevent the wastage of digital evidence. Here, it should suffice to give a real-life example of how a crime can be discovered with the help of digital evidence.

In light of Case Law

According to the facts of a court case in Pakistan, allegation was levelled against a boy that on his visit to his friend's house, he recorded her nude video without consent and shared it to their friend's group on social media. The case was proved on the basis of the fact that the cell phone of the accused remained connected to the internet browser of the victim throughout his stay in her house and the video was made with the mobile phone camera held by the accused at the time of the incident. Additionally, nude pictures were forwarded from this phone to the social media friends of the accused and victim. Clearly therefore, digital evidence can help fight the crime as carrying digital device is now a necessity which very few people can afford to live without.

Necessity of guidelines concerning accuracy, authenticity and reliability

While digital evidence has been subjected to similar rules of evidence as the traditional evidence, does the new amendment actually render it primary evidence.

Has the term primary been used in the sense of admissibility or weight/ appreciation of evidence under the new explanation to article 73 of QSO 1984?

It is important that guidelines for authenticity, reliability and accuracy should be legislated otherwise every lacuna in presenting, storing evidence will leave a dent in the prosecution case because the prosecution must prove its case beyond any reasonable doubt. For instance, how it was extracted, any copy was made, what operations were performed? Is it in its original form?

So, in spite of ETO, still LHC says that an electronic document will be admissible if it can be subjected to cross examination.

Modern day Reliance on Digital Evidence

With the advancement in information technology, the need to rely on digital evidence has increased manifold. In place of paper documents, digitally produced or electronic documents are used. For example, emails have replaced formal and informal letters and applications and even invitations. Similarly, instant text messages have taken the place of voice conversations over phone. Digital photographs are used in place of camera shots of the past. Under the circumstances it became indispensable to make our law of evidence conducive to the requirements of digital evidence.

Putting it simply, our lives have become so much dependent on technology that whoever is living an ordinary life, being connected to the so called global must be using one or the other form of technology. As a result, everyone is leaving digital

traces of the operations they perform on (with) technology. Since in the modern society, all actions involve use of technology, criminals are also putting this to use leaving steps for digital forensics to follow in order to uncover their crimes. For example, a person involved in harassment, child pornography and even kidnapping for ransom is likely to leave digital traces of his or her crimes. However, it was not easier in the past to prove these crimes because our courts used to rely on traditional methods of collecting and presenting evidence which worked well as long as we were dealing with oral or documentary evidence, but they called for drastic changes in admissibility, appreciation and collection requirements the moment digital evidence was introduced.

Objections against Digital Evidence

To begin with, we will try to understand the meanings of digital evidence and other important terms related to this. Digital evidence has been defined as 'any information stored or exchanged in a computer related device and which is in binary form.'

The devices in which such information can be stored include hard disks, floppy disks, memory card, flash drive and the information itself is found in 1's and 0's (binary form) which is not understandable with human faculties. So, the first objection which is raised against digital information is that it's not direct or first-hand information which you can extract from a device rather you would need additional steps to make this information readable such as getting a print out.

Consequences of Electronic Transactions Ordinance (ETO) 2002

However, the promulgation of Electronic Transactions Ordinance (ETO) 2002 has removed this objection. The amendments caused by it clearly suggest that the information extracted digitally whether a document, transaction, communication or audio-visual images exchange cannot be discarded merely on the basis that the same is in digital form. Such evidence is not only relevant but also admissible provided it is direct and not hearsay.

Before the promulgation of ETO 2002, digital evidence was admissible only under one article of the QSO 1984, that is, article 164. According to it, the court may if it deems appropriate allow any evidence to be produced and admitted which is acquired by using modern devices.

Is it hearsay Evidence?

In the like manner, another difficulty with digital evidence has been it being a hearsay evidence of the transaction it purports to record. For example, if an email reads, 'Mr. X will kill Mr. Y' and later Mr. Y is found dead, the email can be primary evidence of Mr. X making such declaration in his email list. However, it is a hearsay

evidence of Mr. X actually threatening B, because Mr. Y is not in the court room where he could be cross examined as to the fact that he heard X making such a claim.

Hence, when digital evidence is used to prove a certain circumstance, digital evidence is direct. However, when it is the sole evidence of the act or transaction which it purports to record, then it will need corroboration from facts and circumstances as well as from other evidence.

Interpretation to the extent of Case law

1. Thus, in an online harassment inquiry, the police found evidence of child pornography exchange, to collect the new evidence, the police had to apply for fresh warrant for seizure of the device.

2. In a famous case reported in a well-known forensic book, the accused was charged with making nude pictures of the victim and then uploading/ forwarding to an email list. The recording found in the accused's phone was corroborated with the fact that throughout the time he remained connected with the phone of the complainant to which the internet was linked.

3. In another case of molestation allegations, the victim stated that she requested the accused to take some of her pictures for uploading on My Space but he molested her while doing this. It was found that the time lapse between first picture and the last picture was 4 minutes & 46 seconds, while the victim stated that the act of molestation was completed in 30 minutes.

Article 5 of ETO Ordinance 2002

Another change that was brought in the admissibility of digital evidence was affected through Article 5 of ETO. This article says, 'if digital evidence is complete and unadulterated, then it will be admissible evidence regardless of the additions caused naturally or by mistake.

Article 46 and Article 73 of QSO

Likewise, Art 46- A of QSO says digital evidence or evidence derived or stored through mechanical process is relevant. This article complements article of QSO which says evidence may only be given with respect to facts in issue or relevant facts. In the same way, an explanation has been added to Article 73 QSO which states that all electronic documents including electronic documents represent primary evidence.

Judicial Pronouncements about Digital Evidence

All these amendments are aimed at fulfilling the requirements of modern-day life style where most transactions are done digitally and even payments are made online, contracts accepted online or deemed to be binding on the parties. However, it is difficult to say that the introduction of ETO and the corresponding changes brought in QSO have changed the status of digital evidence from corroborating to direct or original. While clearly article 73 declares documents produced by applying electronic process as primary evidence, however, it can be argued that the article speaks of computer generated and not computer stored information because further copies can be made out of stored information, still this conclusion requires judicial interpretation because the LHC's Judge Mr. Shahid Kareem has recently held that electronic documents will be treated as a primary evidence subject to cross examination. Furthermore, all over the world there are certain standards of admitting electronic evidence, these include authenticity, reliability and admissibility and fulfillment of these standards necessitates chain of custody, making sure that evidence is not tampered with or destroyed in the process of collecting, who were first responders.

Primacy in regard to admissibility and weight of evidence

Interestingly, all these amendments confirm the admissibility of digital evidence which is a welcome development but they hardly say anything about weight or appreciation of evidence. In order to give weight to the digital evidence at the point of appreciation, it is of critical importance that the evidence should be reliable, authentic and admissible. I think that's where guidelines are needed from the courts of Pakistan. Pakistan is a country following common law system and understandably everything is not given in the statute. In order to understand the wording of the statute common law countries are required to look at court precedents. I think nowhere the need for court interpretation is as intense as in the case of elaborating the ways and means to make digital evidence admissible. Although ETO 2002 and the consequent amendments in the QSO have clarified the primary status of the digital evidence, nevertheless the circumstances are not laid down under which it will be assigned weight.

Guidelines as to authenticity, reliability and originality of Digital Evidence

American Law Reports as well as UK police Chief have developed certain guidelines which must be observed and should be made part of the police rules of investigation. The most important are as under;

1. A record must be maintained of all the procedures applied to the evidence and a copy has been made.

2. Digital evidence is different because it can be destroyed unlike paper shredder. The pressing of delete button does not eliminate it rather it just creates space in the storage device for new chapters or further data input. The detected data can be retrieved by back up operations. Even if the hard disk is formatted, concealed information can be recovered.

3. A third party should be able to apply similar operations which were applied by first responders or forensic experts and get the similar results.

4. All rules regulating traditional evidence should be made applicable to digital evidence. While this has been declared by the Federal Shariat Court (FSC), there have been contradictory statements about the best evidence status and hearsay issues of the digital evidence.

5. A chain of custody should be prepared along with concluding report.

These steps are essential to establish authenticity, reliability and accuracy of the evidence.

All the amendments in QSO resulting from ETO 2002 relate to admissibility of the evidence and not to its weight or appreciation. This assertion draws support from the fact that the amendments focus on computer generated evidence. For example, all computer-generated documents are made admissible by suggesting that these shall not be denied the status of primary evidence because they are computer generated.

Computer stored vs. Computer generated

However, the amendments say little about computer stored documents. While computer generated documents cannot be degenerated by printing copy to copy, computer stored evidence can be subjected to decay, additions and alterations, no policy guidelines exist under the system of Pakistan to prevent this possibility. It is therefore important that either it should be clarified through case law or legislation how the digital evidence shall be extracted, stored and treated in order to add to its weight rather than admissibility. This was one of the reasons behind decision of LHC Judge that an electronic document will only be admissible if it is allowed to be cross examined.

What is required is understanding and statutory acknowledgement of the differences of two kinds of evidence. For example, only a forensic expert should touch it otherwise digital evidence can be adulterated or changed. It would become difficult to attach weight to it if it has been extracted by non- experts. For instance, in the recent case of Noor Mukkadam's brutal beheading and rape, SSP investigation Islamabad

himself acknowledged his heavy reliance on the forensics in a televised interview. He further stated that the evidence is in the custody of the investigators.

Changes brought in QSO through ETO 2021

2 (e): The expression automated, electronic, information, information system, electronic documents and electronic signatures, advanced electronic signatures and security procedure shall bear the meaning given in ETO 2002.

Art 73 (Explanation 3): A print out or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, received or stored in electronic form if the automated information system was in working order at all material times and for the purposes hereof in the absence of evidence to the contrary it shall be presumed that the automated information system was in working order at all material times.

Art 73 (Explanation 4): A print out or other form of reproduction of an electronic document other than a document t mentioned in explanation 3 above, first generated, sent, received or stored in electronic form, shall be treated as primary evidence, where a security procedure was applied thereto at the time it was generated, sent, recovered or stored.

ART 46-A: Relevance of information generated, received or recorded by automated information system while it is in the working order, are relevant facts.

ETO 2002

Sc. 3: Legal recognition to electronic forms

"No document, record, information, communication or transaction shall be denied legal recognition, admissibility, validity or enforceability on the ground that it is in the electronic form and has not been attested by any witness."

Sc. 5: Requirement for original form

i)- The requirement under any law for any document, record, information, communication or transaction to be presented or retained in its original form shall be deemed satisfied by presenting or retaining the same if:

a)- There exists a reliable assurance as to integrity thereof from the time it was first generated in its final form (There's no addition since it was first generated.

It is required that the presentation is capable of being displayed.

2)- For clause (a) of subsection (1).

a)- The criterion for assessing integrity of the document, record, information, communication or transaction is whether the same has remained complete and unadulterated, apart from addition of any endorsement or any change which arises in the normal course of communication, storage or display.

b)- The standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information or communication or transaction was generated and all other relevant circumstances.

Judgement on Video Evidence

In 2021 SCMR 873, the supreme court of Pakistan held that video evidence is an important piece of evidence, however, it can be presented before a court of law if the following conditions are met:

1. Before getting it admitted, exhibited, it will be necessary to explain how was it acquired or what was its origin or source.

2. A forensic report should be presented that the video has not been edited.

Without fulfilling the above conditions, video evidence will have no probative value.

Judgment on Mobile SMS

In the eye of law, mobile SMS is deemed to be a weak type of evidence. However, the in 2021 MLD 1415, the Lahore High Court laid down a new rule. According to it, under article 164 of QSO 1984, SMS record is a strong evidence. This evidence will be deemed as primary evidence which means the court can deliver judgement on the basis of such evidence.

Analysis of the two Judgements

These two judgements have shed light on the importance of digital evidence in modern day world. The first one 2021 SCMR 873 is authored by the supreme court holds that video evidence shall be treated as strong evidence, however, its admissibility is subject to two conditions.

1. Its origin should be accounted for. In other words, it must be explained how the evidence was acquired.

2. A forensic certificate should be presented testifying that the video has not been edited.

Thus, the judgement has enumerated two essential conditions for adding to its weight or probative force. The judgement goes on to explain, without fulfilling these requirements, the evidence will have no value in the eye of law. Clearly, the judgement has identified two important conditions for ensuring authenticity, reliability and originality of the digital evidence. While a number of further conditions are laid down in the UK and US guidelines, although all these guidelines are not mentioned in detail by the Supreme Court, nonetheless, it is evident that Pakistani courts have started focusing on probative value and not merely on admissibility of digital evidence. Of course, with time, more judgements will be delivered highlighting other factors such as chain of custody etc.

The second judgement by Lahore High Court goes a little too far about emphasizing the importance of SMS evidence. There is no doubt that SMS is primary evidence after the promulgation of ETO 2002, so the court's reference to article 164 was uncalled for because this article leaves the admissibility(weight)/ probative force of evidence acquired through modern devices on the discretion of the court.

The court should have referred to ETO 2002 and the amendments caused by it into the QSO 1984.

However, while explaining what primary evidence means that conviction can be solely based on it, the court should have laid down the principles which add to its probative force such as:

i. It should not have been altered.

ii. Its source or origin should be disclosed.

iii. It's not edited.

iv. Chain of custody should be mentioned in detail.

v. Computer generated evidence should be given more priority over computer stored because generated transactions do not allow for copies.

Clearly, now we have laws to support admissibility of digital evidence for example ETO & changes brought by it into QSO. However, what we need is to lay down the guidelines on the basis of which probative force of such evidence can be increased.

This is a welcome development that superior courts have taken upon themselves to identify the factors which add to probative force on legal value of the digital evidence.

Conclusion

This a welcome development that art. 164 QSO has been supplemented by ETO 2002 and the changes brought about it in QSO 1984. What the changes are meant to do is to turn digital evidence into primary evidence. Article 164 QSO made all such evidence relevant which is derived through modern devices. However, the admissibility of such evidence was left to the discretion of the court. In view of this, the courts have been regarding such evidence as secondary evidence requiring corroboration from the maker. For example, if it was audio evidence, the machine recording audio and the person making the recording had to be present in the court. Now, the legislature has categorically declared that any document produced through electronic or digital process shall be treated as primary evidence. Since evidence of the document is quite broad under QSO it includes everything such as writing on floppy disk, hard disk, USB device and anything exchanged over the internet. Previously, the reason for considering digital evidence as secondary evidence was the fact that it requires an additional device such as printer to bring it in a humanly readable form. However, after the aforementioned changes in law, it cannot be regarded hearsay evidence. However, there have been some court judgements which indicate that after the promulgation of ETO 2002, although admissibility of such evidence has become undisputed, however, it will be given more weight at the time of appraisal if such evidence is corroborated by ocular or physical evidence. This line of reasoning needs to be challenged. Hopefully, the more prosecution will rely on such evidence, the better will become familiarity of our judges and the principle will be clarified further that if additions or deletions can be adequately accounted for, and its storage and chain of custody can be explained, it should be treated no different than oral or documentary primary evidence. However, establish such sanctity of digital evidence, Pakistan is required to frame guidelines and rules in regard to storage, extraction, chain of custody, authenticity and reliability of digital evidence.

Recommendations

1. Primacy should be accorded to digital evidence not only in admissibility but also appraisal or weight of evidence.

2. Guidelines and rules should be set forth in regard to storage, custody, extraction, authenticity and reliability of the digital evidence.

3. An expert team of first responders should be prepared in every district who could account for extraction, addition or deletion, preservation, storage, authenticity and reliability of digital evidence.

References

Becker, R. F. (2004). *Criminal investigation*. Jones & Bartlett Learning.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies,* 6(2), 142-153.

Marenin, O. (2004). Police training for democracy. *Police practice and Research*, 5(2), 107-123.

Rabinovich-Einy, O. (2002). Going public: Diminishing privacy in dispute resolution in the Internet age. *Va. JL & Tech.*, 7, 1.

Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT, 1(1), 91-114.*

Singh, R. D. & Aggarwal, N. (2018). Video content authentication techniques: a comprehensive survey. *Multimedia Systems*, 24(2), 211-240.

Umair, S., Björklund, A., & Petersen, E. E. (2015). Social impact assessment of informal recycling of electronic ICT waste in Pakistan using UNEP SETAC guidelines. *Resources, Conservation and Recycling*, 95, 46-57.

Van Dijck, J. (2007). Mediated memories in the digital age. Stanford University Press.

Bakhsh , F, Qadeer Z Abbasi W A . (2020). Legal and Institutional Framework for Prevention of Corruption in Pakistan in Compliance with the United Nations Convention against Corruption (UNCAC). *Pakistan Social Sciences Review*, 4(4), 265-276, doi:10.35484/pssr.2020(4-IV)19

Weeks, J. R. (1997). No Wrong without a Remedy: The Effective Enforcement of the Duty of Prosecutors to Disclose Exculpatory Evidence. Okla. *City UL Rev.*, 22, 833.

White, P. (Ed.). (2010). *Crime scene to court: the essentials of forensic science*. Royal society of chemistry.