P-ISSN: 2709-6254	Journal of Development and Social Sciences	July-Sep 2022, Vol. 3, No.34
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2022(3-III)51	[538-544]

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

RESEARCH PAPER

Recording Evidence through Information Technology and its Implications in Pakistan: An Assessment

[1]Dr. Muhammad Hammad u Salam* [2]Dr. Sardar M.A. Waqar Khan Arif
[3]Dr. Shujaat Ali Rathore

1. Lecturer, Department of CS & IT, Faculty of Engineering and Technology, University of Kotli, Azad Jammu and Kashmir, Pakistan
2. Assistant Professor of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan
3. Assistant Professor, Department of CS & IT, Faculty of Engineering and Technology, University of Kotli, Azad Jammu and Kashmir, Pakistan

***Corresponding Author** hammad.salam@uokajk.edu.pk

ABSTRACT

Evidence at glance is the proof which may be admitted that is both relevant to case in determining whether or not something is more or less true and is reliable, that it can be authenticated. It is explained as a statement offered to prove the words themselves because of their legal effect for this purpose the statement is not considered hearsay. Digital evidence refers to evidence that is not in substantive form, in today's world Computers are manipulated for commission of offence/crime. It is a well-known phrase that "iron cuts iron" here it means that now the law enforcement agencies utilize computers to fight computer generated crimes that are commonly known as cybercrimes. In this context, this paper analyses recording evidence using information technology in Pakistan. The objective is to analyse digital evidence, its kinds and significance of its use. An analytical method will be followed.

KEYWORDS Computer Systems, Digital Evidence, Forensic, Legal Implications, Pakistani Law

Introduction

The term evidence is a multidimensional term and is defined by several authorizes and is spaced in the most prominent dictionaries of the world, some of them are: - A written or spoken statement of facts which helps to prove or disprove something at a trial (Garner, 2004). Absolutely convincing proof is the one which excludes all possibility of error (Black, 1968). That which demonstrates, makes clear, or ascertains the truth of the very fact or point in issue; or it is whatever is exhibited to a court or jury, whether it be by matter of record, or writing, or by the testimony of witnesses, in order to enable them to pronounce with certainty; concerning the truth of any matter in dispute (Bouvier, 1856). The body of rules that governs what can and what cannot be brought before a court in any particular cause. It determines whether and which witnesses may offer testimony and the extent to which they may testify. It is the law of evidence that regulates which writings, printouts, documents or, indeed, other items of real evidence, such as knives, dogs, cars, ships, photographs or videotapes, may be put before the court. It also determines what weight the evidence should have whether it is conclusive, persuasive, indicative or useless. Indeed, it may be said that the known presumptions in law that may resolve a case without any real evidence or testimony are equally part of the law of evidence. The Qanun e Shahadat Order, 1984 (QSO) provides a detail account of the definition: evidence includes: All statements which the court permits or required to be made before it by witness, in relation to matter of fact under inquiry, such statements are called evidence. All documents (including electronic record) produced for inspection of court such documents are called documentary evidence (Sec 3).

If we summarize the term evidence in the language of court than it can be defined as the examination-in chief and cross examination on that examination in chief is called evidence.

According to Sir Stephen the term evidence is ambiguous one. He holds that in some cases it means the utterance of witness before the court of law; in other cases the utterance that prove or disprove a case before the court of law; and in some cases it also means that a particular fact narrated before the court is relevant to the issue that is pending before the court to be sorted out. Another definition that is given by online sources is "the proof which may be admitted that is both: (a) Relevant to the case is determining whether or not something is more or less true, and (b) Is reliable that it can be authenticated (Collins Dictionary). This paper is divided into V Sections. Section I is introductory. Section II analyses definition of the digital Evidence. Section III analyses kinds of digital evidence. Section IV explains significance of digital evidence and implications. Section V analyses valid digital devices. Finally conclusions are drawn up.

Digital Evidence and Information Technology: Definition and Literature Review

Digital/ electronic evidence is basically the information collected or communicated in binary form that can be produced before the court of law and the court may rely upon on such piece of evidence. It has several places to hide itself, like it can be found on a computer hard disk, a mobile/cell phone, a Compressed Disk (CD), and a pan-derive etc. Digital evidence is generally connected with electronic crime (e-crime) such as fraud committed through Automated Teller Machine (ATM), child pornography hacking etc.

Another definition is given by Scientific Working Group SWG by using these words "Digital Evidence is any information of probative value that is either stored or transmitted in a binary form, Later "binary" was changed to "digital". Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. The information that is electronically taken up (seized), collected, stored, processed, authenticated and preserved for presentation before the court of law during the proceedings of trial of the offence, the only check, on the above steps is the proper obedience and observance of the provisions of law dealing on the subject (Casey, 2000).

In order to fight with the offenders of electronic/digital crimes and to investigate, law enforcement agencies are integrating the collection and analysis of digital evidence that is known as computer forensics, into their infrastructure, here forensic refers the application of scientific methods and techniques that are utilized in a course of investigation of a crime. It is evident from the above literature that it is not easy to propose a uniform policy upon the issue and expect the fruitful results from the world, because every country has its own legal environment, the substantive and procedural laws vary from state to state, they are very specific and environment-oriented (Walden, 2017).

As far as contribution of Pakistan in such an important field is concerned, the main law that is being functional in Electronic Transaction Ordinance (ETO), (2002), which have a detail account of digital offences and somehow contains the technique to take-up the same. The main development in this field is the modifications to the Qanun-e-Shahdat Order, (1984). Another development in the banking side is Finance Institutions (recovery of Finance) Ordinance, (2002), the digital crimes are being defined in the Prevention of electronic crimes Act, (2016), and procedural glance is presented through enactment of Investigation for fair trial Act, (2016) and rules, (2016). The ETO has given space to the information in digital form to be presented before the court of law and it could not be denied, as the Preamble clarifies the purpose in these words:-"the ordinance to recognize and facilitate the documents, records, information's, communications and transactions in electronic form and to provide for accreditation and certification service providers" (The ETO, 2002 Preamble).

Kinds of Digital Evidence and Information Technology

As far as the kinds of evidence present in electronic devices like computer are concerned, we may find several evidences in computer when it is compromised or manipulated, these evidences may have several places. Following are some kinds of evidence which one can obtain from the computer:-

Computer Logs

Computer logs are defined as the documents prepared by the user in the computer, it may include the documents in form of Microsoft Word (MS Word), excel, power point, text, graphics, multimedia. These files are the part of computer memory and are itself a digital evidence as system logs, these files may be extracted and retrieved from their location in the computer, the only thing that matters here is the storage, it means that how such date is being stored, where the particular data situates, how that device managed the stored data.

Formation and Modification of the Documents by Computer User

This point involves two mainstreams one is creation or formation of data by the user, it means the date and time on which a new file is created by the user and the other is using possible tools to find the data available in the computer. Every data involved in the search of data is called metadata, in simple words metadata is the clue of available date e.g. search of a file by using some letters or number, this search is itself a piece of evidence that can be collected by experts, by using special tools, techniques and digital mind.

Program File

Program in the language of computer means the sequence of instructions given to the computer to do a particular task and the file which contains the instruction for Central Processing Unit (CPU) is called program file. One may take advantage of program while investigating the computer. In a quite simple sense the location of data in disk is organized by a file system.

System File

A system file can be defined as the file in computer that holds data about the computer's basic operations. The absence of system file may cause inefficiency in the functioning of computer, it may cause a computer black out.

Temporary Files

Temporary files are the files that have a short span of time, e.g. Random access memory (RAM) is responsible for memorizing the initiated. From the above discussion it is concerned the prime focus is to find out the places within which the evidence is hidden and what help the investigator while investigating a computer.

Significance of Digital Evidence in Current System

Digital evidence is the most diverse kind of evidence in the modern world, there may be three or four identities for digital evidence, like electronic evidence and computer evidence etc. Digital evidence is a bilateral term and is composed of digital that means having digital essence and evidence is obvious. The term digital is extracted from the term digit, which means number. The term digital refers to being data in form of digit, characterized by electronic and especially computerized technology (Webster, 2019). The term evidence has previously been defined as any information that can be produced before the court, on which it can relay and sorted out the matter in issue (The Evidence Act, 1872 3).

The simplest definition of digital evidence is the evidence stored or transferred in form of binary (the language understood by the computer) on which the court may relay to decide the case. By comparison of both of the terms digital and binary, we came to know that

the term binary is very limited and restricted term that only indicates and represented one form of data, which is binary while the term digital has more exposure and diversity than the term binary. It enlightens any kind of data in digital format.

Now a days digital evidence is most comprehensive term and cover almost all kinds of the evidence generated by any digital device, in previous time it is just confined to the evidence generated by and from the computer, now the definition of electronic evidence cover almost all the devices that are been made by humans, the information generated, stored and transmitted by them, and do have the potential to describe its nature and enable the investigator to take up the same and brought it into the shape which can be presented before the court. By explaining the above said definition it seems that there are certain dimensions of the digital evidence, in the beginning it gives space to all available forms of evidence that are created, manipulated, stored, transmitted and transferred from one device to another device in any form, the scope is so broader that it just exclude the human brain from the said definition (The QSO, 1984 Art 164).

A quotation for the parliament of United Kingdom (UK) is very much important to mention, that it has the power to enact and amend any law rather to change or amend the laws and trends set by Devine authority, by comparing the said quotation with the definition of digital evidence, it has now give space to all form of evidence generated, stored, transmitted by all the digital devices including computer, mobile phones, scanners and cameras, automated systems etc. In early times the fountain of digital evidence was the only computer, the modern time and modernity, in offence changed the trend, now all the digital devices capable to generate, store, transmit, translate and transport the data or information are termed as digital devices/instruments.

The question regarding the admissibility of the information generated and stored by digital medium raised, that is answered by the legislation in the words and is also complemented by the judiciary of the world, it is now a well settled principle that evidence generated due to digital devices is admissible piece of evidence before the court of law (The QSO, 1984 Art 164). Domestic as well as the international conventions are now in support of digital evidence. The criterion for admissibility differs from case to case, "admissibility" is not included in the definition because the scope of admissibility is as much broader term digital evidence itself, the criteria of digital evidence differs from country to country, based on their domestic legislation. Thus digital evidence in Pakistan is admissible.

Discussion and Findings

Valid Digital/Electronic Evidence in Pakistan

As far as the question of validity of digital evidence is concerned, it seems that almost whole world is now enriched with the laws that enlighten the digital evidence and consider it as the admissible piece of evidence, the court can rely on it to decide the case, the reliability of the court on digital evidence may differ from case to case. As far as the definition of admissibility and reliability is concerned admissibility here refers to admissible piece of evidence, it may refer to the evidence that may be considered by a trial court as the rules of evidence deem it reliable and relevant. The reliability in this perspective deals with the reliable digital evidence, the criteria for reliability of digital evidence are prescribed in different statutes of the world. The United Nations Convention on the use of electronic communication in International Contracts, (1996), the United Nations Convention on International Trade law (UNCITRAL) UNCITRAL Model Law on Electronic Commerce, (1996), United Nations Commission on International Trade Law (UNCITRAL) Model Law on International Commercial Arbitration, (1985) are the International documents enlightened and enshrined the admissibility and adoptability of the digital evidence as an admissible piece of the evidence. Article (Art) 9(1) specifically endorse the digital evidence as admissible form of evidence in any legal proceedings (UNICTRAL, 1966 Art 9 (1). Art-9 flourished digital evidence by enlightening the weight of the data massage, it means that the

data massage/data or evidence in digital format cannot be negated from its due worth merely on the ground that it is available in digital format. The area of investigation, collection, preservation, transmission, presentation is different from country to country investigative process. The digital data taken up from first stage may change its shape because several methods and techniques are adopted to preserve it and convert it in a shape that can be brought before the court of law for deciding the case, Art-9 also provide shelter to this process because digital data is processed intensely through intense techniques and methods it may change its shape, it cannot be denied in legal proceedings as admissible piece and having a weight.

The other landmark on the same issue is United Nations Convention on the use of Electronic Communication in International Contracts, (2005) (UNECIC) made electronic communication as an admissible evidence in the International Contracts, it means digital evidence is admired and admired from the flour of United Nations (UN), the UN taken up the issue of digital evidence seriously and proposed the conventions to cover each perspective of the digital evidence as admissible piece of evidence in order to guide the states to propose domestic laws and to give space to the digital evidence as admissible form of evidence. The UNECIS is specially designed to complement the laws and trends of Electronic-Commerce (e-commerce) (business conducted online or via the use of computer and without paper). The convention's prime focus is on the communication in electronic/digital format and to deal it as admissible piece of evidence in the premises of any court. It gave a wide range of diversity between the digital language and the digital documents (UNECIS Art 2, 12). As the UNCITRAL model describe the admissibility of the evidence in digital format, the UNECIS clearly described that the electronic communication cannot be denied as admissible evidence solely on the ground that it is in digital format.

In a simpler language UNECIS covers the digital language from each perspective to declare it is admissible in order to curb the tensions arisen after globalization of the world and its business. Digital language is now a part of domestic evidence laws of the world, many countries have already adopted the abovementioned conventions and adopted in their domestic legislations to deal the issue locally. The term Electronic signature E-Sign is also covered in other UN documents, meanwhile the e-sign is also declared as the admissible object to be presented and appreciated by the courts of law. E-sign is defined as using the digital and paperless methods to sign a document, there are several methods describe the guidelines and available trends on the e-sign, e-sign is as binding as, the formal written signature is binding and presentable and relied upon by the courts. The conventions also established a convenient system, it allows the parties of the contract to alter the terms and conditions as agreed upon by them.

The Council of Europe Convention on Cyber Crime, 2001 (CECC) which has its special name *Budapect* is the first ever landmark, an internationally binding legal mechanism that enlightened the outcomes of Information Technology (IT) for the substantive and procedural criminal laws, the basic theme of the convention is to highlight the worldwide enforcement and execution of law in cyberspace, cyberspace is hereby defined as non-physical space that exists between computer nodes (The Budhapect Convention). The contribution of UN in the field of digital evidence is phenomenal, UN tried to propose the International Conventions on the said issue which is now converted into a worldwide issue, UN gave guidelines to the member states to complement the conventions of UN by adopting the conventions and enacting the domestic laws having the common theme and motive. It is the outcome of the above-mentioned convention that the third world countries like India, Pakistan and Bangladesh, etc. are now having their enacted domestic laws that are continuing a positive result.

It is very easy to understand by reviewing the current stance of the world on digital evidence and its admissibility discussion, the issue of digital evidence and its admissibility is a worldwide issue because in this time of IT the offence is borderless, it means it can be

committed by a person residing in the east of the world and the offence is being executed in the west of the world. Here the question of Jurisdiction of the Court to whom the matter would be brought for decision arises, the answer to this question is very simple, UN proposed and passed the convention to address the issues and guided the world to adopt the same and propose legislation as per the convention so that the state would be enabled to try such offences and penalize the culprits as per the provisions of the law.

In Pakistan the main benchmarks endorsing the term digital evidence are The Electronic Transaction Ordinance, (2002) (ETO), amendments in Qanun-e-Shahadat Order, (1984) (QSO) and the benchmark judgments given by honorable judiciary in this perspective. In simple words Pakistan is now on the point where it will reach soon to a reasonable conclusion.

Conclusions and Recommendations

From the above discussion it is concluded that recording Digital evidence through Information technology is now rooted in almost all the judicial systems of the world due to modernity in committing the offences, now the offence is boarder less and is more severe as compared to a formal offence which is committed against the society, the cybercrime is the crime against the word, the only way to punish the culprits is to legislate domestically and try the offences, it can only be possible when you have the law that guide the law enforcement agencies how to investigate the offence, how to collect the evidence that are not in substantive form, how to convert the information into the language understandable for judiciary. Recording Digital/electronic evidence through Information technology is effective in inclusive range of investigations including sexual offences like child pornography, homicides, women and child abuse, harassment, drug dealing, hacking and stealing the servers, fraud by using digital mediums. It is also effective in civil cases. The records in digital form can assist the court to establish a view about the events that had happened. Recording of Digital evidence through Information technology is admissible in the Courts of Pakistan. However, the implementation of laws in letter and spirit is a big challenge. This paper recommends that use of digital technology is essential for nation building. It is important to consider growing technology in different institutions/sectors of Pakistan.

References

Black, H. C. (1968). Black's Law Dictionary; definitions of terms and phrases of American and English jurisprudence, ancient and modern.

Bouvier, J. (1856). *A law Dictionary, adopted to the law and constitution of United States* , Book on Demand Ltd

Casey. E. (2000). *Digital evidence and computer crimes*. Elsevier

Definition; evidence'thelaw.com dictionary, https://thelaw.com/definition/ evidence

Garner, B.A. (2004). *Black's law dictionary*, Thomson West

Indian Evidence Act, (1872). Sec 3

Malik, N. A. (1984). The Qanun e Shahadat order

Stewered, W. J. & Burgess, R. (1996). Collins Dictionary Law, dictionary of law.

The Electronic Transaction Ordinance, (2002). Preamble.

The Evidence Act, (1872). Art 3.

The Qanun-e-shahadat Order, (1984). Art 164.

The United Nations Commission on International Trade Law (UNECIS), Art 2 10 12.

The United Nations Commission on International Trade Law (UNCITRAL), (1966). Art 9 (1).

Walden, I. (2017). *Computer crime and digital investigation*. Oxford University Press