Hafsa Abbasi*
Muhammad Asim Iqbal**

Authentication of Electronic Evidence; A Journey from Electronic Discovery to Digital Forensic Experts in Western Law-Recommendations for Pakistan

ABSTRACT

This article claims that electronic evidence is not like physical evidence and requires some more guarantees of authentication which are not required otherwise. Electronic evidence needs some extra precautions to be taken care of during discovery and authentication procedures. Electronic discovery and authentication are inevitable procedures involved in electronic evidence trials, posing different challenges of electronic data and expert testimony therefore need to be ascertained from the perspective of Western as well as Pakistani law. Getting authentic and fool proof evidence to court is an important research question addressed by this research. Digital forensic experts are essential to carry on these procedures. Qualification of digital forensic expert is also important to be ascertained for seeking reliable evidence. Western laws are incorporating suitable laws and policies in order to cope up with the upcoming challenges of big data, management problems and preservation of ESI (electronically stored information). This research concludes that there is a need to upgrade laws and policies of Pakistan, which regulate authentication, discovery and expert testimony, as they are at very primitive stage.

Keywords: *Electronic Discovery, Evidence, Spoliation Authentication, Data*

Introduction

Advancement in technology has had a huge impact in all fields of life. Computer revolution has indeed increased the productivity of institutions.

* Lecturer, Department of Law, Allama Iqbal Open University Islamabad, Pakistan
** Assistant Professor, Department of Law, International Islamic University Islamabad, Pakistan

Shifting from paper documents, to electronic systems has reduced the costs and is helpful in meeting challenges quickly. Computers have posed real differences in the process of litigation too, the data stored on a computer is digital and different from manual business record which lacks many of the guarantees of reliability found in traditional methods of record keeping. Computerized information can be distracting or confusing for the judges and lawyers. Article 164 of the Qanoon-e-Shahadat Order 1984 provides that "in such cases as the court may consider appropriate, the court may allow to be produced any evidence that may have become available because of modern devices or techniques". This offers possibility of dealing with huge voluminous data, as well as increasing the possibility of disclosing private information. (Long, 1986).

These investigative and reliability issues are solved by employing latest techniques of electronic discovery and authentication. Collection, examination and authentication of electronic evidence has become latest science these days. Electronic discovery is conducted for extracting useful information and dealing with huge data. Discovery is a part of preparation for trial where parties are under obligation to exchange relevant information to each other (Daniel & Daniel 2012), Sometimes thousands of emails and documents are exchanged between the parties as many employees use emails, messages and social media to communicate.

The purpose of effective electronic discovery is to attain authentic evidence. Authentication of electronic evidence is the most crucial stage of admissibility. If there are little doubts in the integrity of evidence court rejects that evidence. Laws and principles of western countries in the areas of discovery, authentication and expert testimony are very well established, therefore, there is need to analyse them in order to explore the examples for improvement in laws of Pakistan, which needs upgrading. Different countries are legislating and making policies to utilize the modern technology at its fullest and minimize the problems. Pakistan is also trying to grapple with these laws to avoid problems. (Ricea 2005)

Present research shall mainly focus on investigation of electronic evidence through electronic discovery procedures. It will elaborate further the requirement of preservation and privacy in case of electronically stored information. Then authentication methods of electronic evidence shall be discussed at length it will highlight the latest advancements in western law on the topic of authentication. Since authentication and discovery are not possible without experts so the criteria of qualification of digital forensic experts shall be discussed in western law. Then stance of Pakistani law shall be explored.

Investigation of Electronic Evidence; Electronic Discovery

Electronic discovery is actually a pre-trial discovery of electronic evidence before trial. It involves search of different sources like websites, emails, USBs, backup tapes, servers etc. It is also called document discovery or Electronic Data Discovery (EDD). It means "any process (or series of processes) in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. Another type of e-discovery is court-ordered investigation or government sanctioned inspection. It can be carried out offline on a particular computer or it can be done across a network" (Conard, 2017).

There are e-discovery soft wares available in market which are quite useful in collecting, extracting and organizing the data from all kinds of servers and devices. Such techniques and soft wares are be used by attorneys in order to redact personal information, which includes company secrets and the privileged communication before giving the data to the opponent party. Furthermore, the attorney can also use this technology to tag "relevant or not relevant document." *(Ralond, 2007)*

One of the major differences in manual document discovery and electronic document discovery, is lack of an audit trail[2]. Any information can be deleted from a data base without leaving any traces.[3] Circumstantial evidence will be helpful to verify the information present in a system. In the absence of an audit trail, methods of data input and retrieval processes matter a lot. Any weakness in the above-mentioned methods shall prove to be a hurdle in admissibility and credibility of electronically stored information[4] (Long 1986).

However, still the chances of evidence being destroyed or lost are higher in civil cases than in criminal cases because in civil cases the parties may know that they will be asked to disclose the evidence to the other party. Therefore, he may dispose of anything which is incriminating. On the other hand, in criminal cases the evidence is typically seized without any forewarning of destruction of evidence (Daniel & Daniel 2012). The punishments for destroying or alteration (spoliation) of electronic evidence are quite high.

Requisites of discovery

[2]Audit trail can be defined as, "a record of a sequence of events (such as actions performed by a computer) from which a history may be reconstructed". *Merriam Webster s.v Audit Trial*. https://www.merriam-webster.com/dictionary/audit%20trail

[3] However, there are technologies which can retrieve deleted data.

[4] Richard m long, E discovery and Use of Electronically Stored Information, 5.

As stated above there are two pre-requisites of electronic discovery, preservation and privacy. Lack of proper preservation can heat up the issues of management, spoliation and cost etc. Privacy, on the other hand, if not ensured properly, can raise the issues of privileged communication. If any of the conditions mentioned above are not fulfilled properly, the evidence will lose authentication and will face rejection from the court.

Preservation

Well preserved electronic data is very important for seeking authentic evidence. Parties are bound to preserve data when it can foresee that such data will be required in litigation. The main essence of preservation is to keep the data in a form which can gain trust of court, i.e being free from all errors and is reliable. But demand of document, in a lawsuit, must be reasonable. It is discouraged to demand irrelevant huge amount of data for burdening the other party.

Preservation duty is recognized by the majority of institutions dealing with electronic evidence. One of the example is of ACPO guide, which states that;

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result (ACPO guide 2011).

Preservation shall be complete and effective, if proper trails and chain of custody logs are maintained. These logs identify the least alterations. Logs are like hash tags which are unique numerical identifiers and can be assigned to a file, based on algorithms. These values will be so distinctive that the chances of having two data sets same value are one in billions.[5] Any third party can process and achieve the same results. It is being clearly mentioned that the process of preservation should be completely fool proof and effective. So if it is examined by a third party the same results can be acquired.

[5] It means "A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values, so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production." Rothstein, Barbara Jacobs, Ronald J. Hedges, and Elizabeth Corinne Wiggins. *Managing discovery of electronic information: A pocket guide for judges* (Federal Judicial Center, 2007), 24; see also Williams v. Sprint/United Mgmt. Comp., 230 F.R.D. 640, 655 (D. Kan. 2005).

In other words, evidence must be preserved in a state which is defendable. Most important thing in the process of preservation is flawless chain of custody. [6] In case of any breakage in the chain the reliability of evidence will be doubtful. Another important thing is to keep the evidence safe from malicious tampering, destruction of evidence and accidental modifications from untrained persons. "Chain of custody logs" are generated to solve these problems. These logs must include every instance when a piece of evidence was touched, like, the time of initial collection of devices storing the evidence, the transport and storage of evidence, and all the times when evidence was checked out for forensic examination or other persons (Daniel & Daniel 2012).

The consequence of not being able to comply with the requirements of preservation are sometimes very grave. There are lots of cases when parties had to bear heavy sanction for not preserving the required data. Zubulake case. *Eckhardt v. Bank of America Corp.*, 2008 WL 1995310 (W.D.N.C 2008)

The sanctions imposed on the parties include;

i. Monetary fines of millions of dollars.
ii. Adverse inference instruction to juries in cases that later resulted in substantial verdict.
iii. Default judgments on the merits of disputes (Roland, 2007).

Scope of electronic discovery is also an important thing to be kept in mind. For example, how much data should the parties save and what should be deleted in the ordinary course of business? Parties are generally bound to save all the information which is anticipated to come under any trial. It includes admissible data which can be requested to be handed over during discovery.

However, this does not mean that parties should be forced to go through extra ordinary measures. As it was observed in case C*onvolve, Inc. v. Compaq computer Corp* 223 F.R.D. 162, 175 (S.D.N.Y. 2004). 66, that "there is no duty to preserve if it requires heroic efforts, far beyond that those consistent with the responding party's regular course of business". Courts justified this principle by saying that "preservation of every email, electronic document every back up tape would cripple large corporation who are always involved in litigation."

After highlighting the rule above, in C*onvolve case,* court concluded that "there is no duty to preserve a particular wave form or trajectory present in a drive head as no business purpose ever dictated the data's retention. The data was relevant only to damages and the data's relevance in proving the other party's claims could be proven through other means."

[6] Chain of custody means the document must be present in reliable custody. It contains a chain which proofs that at no time, the record or data was left in an unreliable custody which could tampered or affect the integrity of that evidence.

(Roland, 2007).

a) Data

Organizations during preservation is to deal with huge voluminous data, multifarious sources[7] and nature of electronic data. Like, DVD, USBs, SD card, backup tapes, servers and data basis. *Sony Music Entertainment Ltd (Australia) v University of Tasmania* [2003 FCA 532

Electronic data during trial investigation is highly complex. It consists of large amount of structured and unstructured data, all intermixed with variety of file systems, media systems, devices and media types. Along with that the increased use of cloud stored data and other factors increase the volume of data too (Quick & Choo 2016).

b) Cost

Another challenge, other than complexity of data and sheer volume is the cost. Electronic discovery procedures are becoming more expensive each day. Generally, courts mitigate this problem by putting cost on the party who is seeking the information. *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S (S.C) 30 (1982). Sometimes courts shift most of the cost of e-discovery on the plaintiff. For instance, in case *Wiginton v. CB Richard Ellis, Inc.* the plaintiff requested that the defendant should bear the cost of discovering 94 backup tapes, for relevant evidence. The plaintiff supported the argument by telling the court that 3 backup tapes had big amount of relevant data. Defendant argued that the relevant data from the searched backup tapes is very small and that the plaintiff should bear the cost. In order to analyze who should bear the cost, court applied *zubulake* test, 220 F.R.D. at 217. The court decided that, to weight "the importance of the requested discovery in resolving the issue at stake in the litigation". Balancing these factors court decided that plaintiff would bear 70% of cost and the remaining cost will be borne by the defendant party.

c) Spoliation

Spoliation includes destruction of evidence by the parties, which is either relevant or is either destroyed in contravention of duty to preserve. It was observed in case *William T. Thompson Vo. V. Gen. Nutrition Corp,* 593 F. Supp 1443, 1455 (D.D Cal 198), that "court has authority to impose sanctions on a party that destroys documents, that is known or should know will be relevant to the legal action". Similarly, in *Linen v. A. H Robins Co,* 97-2307, 1999 WL

[7] Sources of electronic evidence are many. For instance, emails, text messages, back-up tapes, excel files and internet postings etc.

462015, at * 11, it was further stated that "spoliation of evidence occurs when there has been negligent or intentional destruction of physical evidence which result in some unfair prejudice to the opposing party" (Redish 2001).

Pakistani law is silent on the major issues of spoliation and even electronic discovery. [8] Section 94 of Crpc and Section 30 of CPC deal with discovery but none of them address electronic discovery. These section deals with the physical document discovery and electronic discovery is not discussed in it. Most of the cyber cases, these days deal with electronic discovery so this area must be properly dealt in the laws of Pakistan.

Such problems need to be addressed in Pakistani law as well. Things yet to be clarified by Pakistani courts are that when the duty to preserve arises, or level of requisite knowledge of the party who was involved in destruction of evidence. Serious problems can be faced in case evidence is not duly preserved. For instance, in both "*Khanani and Kalia*" Ishaq Tanoli, (2019) and "Axact" case., (Walsh, 2015).

The major problem faced by the courts were destruction of relevant evidence (spoliation) and lack of relevant laws in order to penalize the offenders.

Electronic evidence is given a prime importance in Pakistani cases and courts. During pre-trial investigation laptops, mobile phones and other electronic gadgets are confiscated by the accused parties. Forensic reports and expert testimony are a matter of routine in cyber cases conducted at special courts of Pakistan.

d) Management Issues

Management of electronic data is another problem. There is confusion about who should be responsible for the record retention and deletion policy. Person developing and monitoring the policy is not defined as well. It should be clear that who would be the authority or who would monitor the policy and who should be an authority. The majority of the companies assign the whole responsibility to their IT department with little or no training on the legal requisites of electronic document retention and deletion. Generally, due to lack of training on the part of employees, they do not submit all the required data. Employees usually misunderstand the requested documents as

[8] The Pakistani law for dealing with Electronic Discovery are the ones which deal with general document discovery. Such as section 94 of Cr. Pc, states "Summons to produce document or other thing.-(1) Whenever any Court, or 1* * *, any officer in charge of a police-station considers that the production of any document or other thing is necessary or desirable for the purposes of ,any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it or to produce it, at the time and place stated in the summons or order."

only those which are ready for the business purposes and do not consist of emails to co-workers, PDA's, blogs, or private meeting notes. If such information is not produced on demand, the companies are at a risk of sanctions imposed by courts. (Redish, 2001)

Archiving of documents is not the responsibility of IT department. It is the responsibility of management to ensure that an adequate retention policy is developed and executed. Management must ensure that approved procedures are followed properly. IT department is frequently charged with providing archival solutions but they cannot succeed without the support of management. (Martin and Cendrowski 2014) Otherwise if the documents required is deleted or not available court will punish the organization with heavy fines. It is generally assumed by courts that deleted data is removed deliberately for fear to produce in court.

Privacy

Another important measure for electronic discovery is to maintain privacy. Big organization have a huge amount of private data containing their trade secrets or other privileged communications. In this regard many protective orders are a matter of routine. There orders include: the data will only be used for litigation purposes and will be destroyed at the end of trial (Isom 2006). Or parties after receiving any private data are bound to return.

a) Privileged Communication

As stated above that privacy is another of the most important requisite of electronic discovery expeditions. In case of failing to comply with privacy requirement, the evidence can be rejected. One of the ground of rejection can be privileged communication. It is, "confidential communication". The issue of privileged communication can be vital in case of electronic discovery process. It aims to protect parties form incrimination where conversation has taken place between relationship that are built on trust and confidence and was made with an intention to be kept secret.[9]

Authentication of Electronic Evidence

Authentication of electronic evidence means evidence must be proved beyond reasonable doubt. This requirement is intended to exclude the unreliable information. Proponent must offer evidence "sufficient to support a finding that the matter in question is what its proponent claims." (Judish, 2009).

[9] Qanoon-e-Shahadat order 1984, also recognize privileged communication in Article, 9 and 12. These privileges include solicitor-client privilege, litigation privilege etc.

Authenticity as already discussed is the means of proving the document to be what it is purported to. The document should be proved to be genuine. It has a vast scope. The subject matter of authentication includes techniques to preserve data and its protection from being manipulated or altered wrongfully. These methods include providing audit trails of transmission[10] and maintaining records of encryption.[11] These techniques are to be applied during discovery and search and seizure of digital data. The document to be authenticated in the court must comply with the claim that it was duly preserved and is free from any manipulation and corruption (Volonino & Anzaldua 2008).

A number of factors provide the evidence of authenticity for such records. Mode of preservation, guiding statutes and forms of transmission maintains the authenticity. The method of preserving the data and the way it is managed also plays a great role in the maintenance of this claim.

Authentication ensures, complete trust or distrust of the judges on the evidence. Therefore, the right evidential foundation, for proving authentication, is essential or else the case would be at stake, and so would be the interest of parties.

Electronic data cover a wide range of reliability scale. There is a difference between authentication of computer generated electronic evidence and computer stored electronic evidence. Computer generated evidence, prepared without human intervention is presumed to be unbiased and accurate, (Reidy et.all 2007), as long as the computer is working properly. On the other hand, computer stored evidence like, instant messages logs can be very easily manipulated or altered similar to emails. The reliability and authenticity issues are further complicated when preparing to produce electronically stored information (ESI) in court. For instance, opening a Microsoft Word document for the sake of printing or imaging effect changes from the original, including creation of new metadata (Palage & Cona 2001).

Computer stored records involve human input and statements. That is why their authentication involves proof of the reliability upon the statement. Oral testimony is the first tool in authentication of such documents.

---

[10] Audit trail (also known as audit log) is a security relevant chronological record that provides source and destination of records for documentary evidence of the sequence of activities. It is helpful when such activities have affected specific operation, procedure or event, at any time. The process which run audit trail should be run in a mode which can access and supervise all actions from all users. But a normal user should not be permitted to stop or change it.

[11] Encryption means translation of data into secret code. It is the most effective way to achieve security of the data. The reading of an encrypted file requires access to a password or secret key that enable to decrypt it.

Authentication Methods

Hash tags, meta data, circumstantial evidence, Oral testimony and expert testimony are the most significant tools for authentication of electronic evidence.

a) Hash values[12] can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication. Hash values can be used during discovery of electronic records to create a form of electronic "Bates stamp"[13]

b) Another way an electronic evidence could be authenticated is by examining the metadata for the evidence. Metadata is commonly described as "data about data," and is defined as "information describing the history, tracking, or management of an electronic document. Phillip J. Favro, (2014). In *Re Telxon Corp. Securities Litigation* **133 F. Supp. 2d 1010 (N.D. Ohio 2000),** the judge highlighted the defendant's failure to present metadata as a basis for the decision. In this case, the defendant omitted the metadata which concealed the modifications made to his record. The record file history showed that the defendant had altered some documents after being ordered not to do so. This resulted in the imposition of sanctions. It is a duty of the involved parties to present documents properly and conceivably produce the metadata.

   Another case *Hagenbuch v. 3B6 Sistemi Electronic S.R.L* (2006), in which the court held both the parties under an obligation to produce documents in their native format which ensured the production of their metadata. Court observed that, "It is clear that the TIFF[14] documents do not contain all of the relevant, non-privileged information contained in the designated electronic media." That is why the documents could not be authenticated and was rejected.

c) Another strong source of authentication of electronic evidence is by way of circumstantial evidence. These are other hints, or clues which prove or

---

[12] As defined above in para 2.1.1

[13] Bates stamping is the process of applying a set of identifying numbers to a document collection of PDFs to label and identify them. You can use Doc Previewer to apply a Bates stamp to documents — even if you don't import them into a case spreadsheet. for example, during the discovery stage of preparations for trial or identifying business receipts. Bates stamping can be used to mark and identify images with copyrights by putting a company name, logo and/or legal copyright on them. This process provides identification, protection, and automatic consecutive numbering of the images

[14]TIFF (Tagged Image File Format) does not contain metadata. Unlike the original electronic media, the TIFF documents do not contain information such as the creation and modification dates of a document, e-mail attachments and recipients, and metadata

disprove the facts. For instance, in *U.S v. Simpsons*, 252 U.S. 465 (40 S.Ct. 364, 64 L.Ed. 665) the defendant objected that the conversation between the defendant and the FBI agent was not properly authenticated. Since government was unable to identify the statements attributed to the defendant through his voice, style or handwriting, the court rejected the plea and observed that government authenticated the chat room printouts by a number of other circumstantial evidence. For instance, during the discussion in the chat room the defendant mentioned his name, street number of his residence and his email address. Later on, during a search of the defendant's house, a page was found near his computer mentioning his email address, street number and telephone number which was given to FBI agent.

d) Oral Testimony is another one of the major sources of authentication. Courts have acknowledged in many cases that documents may be authenticated through oral testimony i.e. by the personal knowledge of the witness. For example, in the case of *United States v. Kassimu*[15], 1880335 (5th Cir. Jul. 7, 2006), the court ruled that the copies of the post office's computer can only be authenticated by a custodian or other qualified witness who had personal knowledge of the procedure that generated the records.

   Generally, witnesses who testify to the authentication of computer records need not to have special qualifications. In most cases, the witness does not need to have programmed the computer himself or even understand the maintenance and technical operation of the computer. The requirement of knowledge can be constructed liberally. It can be said that witness had the knowledge when he actively participated in the event or observed the event.

e) Expert Testimony is essential for electronic evidence due to its technical nature.

Authentication of Electronic Evidence in Pakistani Law

Section 5 of Electronic Transaction Ordinance states that;

"1) 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 the integrity thereof from the time when it was first generated in its final form; and (b) it is required that the presentation thereof is capable of being displayed in a legible form.

[15] 2006 WL 1880335 (5th Cir. Jul. 7, 2006)

(2) For the purposes of clause (a) of sub-section (1);
   (a) the criterion for assessing the integrity of the document, record, information, communication or transaction is whether the same has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display ; and (b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information, communication or transaction was generated and all other relevant circumstances. "

Clause 1 mentions that documents or communication is considered original if there is a reliable surety about its integrity. It means that when it was generated for the first time, after that time there must be surety that since then it is under safe custody. Method of seeking reliability is not mentioned. Fragile nature of electronic evidence suggests that it can be altered very easily. [16]

It is to be noted that subsection 2, clause b mentions that the ascertainment of integrity of electronic evidence shall vary according to type of document. It has mentioned different types of documents i.e, communication, transactions, record and information. But it has not differentiated between computer stored and computer generated evidence.

Likewise it has not mentioned hearsay rule regarding computer stored evidence as well. It has been mentioned that the document has remained complete and unaltered, apart from the changes arising in the normal course of communication, storage or display. This section does not define what the course of communication is. The method of proving a document incomplete and unaltered remains ambiguous.

Such problems are addressed in the laws of other countries. For instance, in the USA's law of evidence, they have clearly mentioned that they would assess the integrity of a document with the help of hash values. In US codes, Code no. 44926, it is clearly mentioned that the document shall be maintained and secured by encryption and hashing. Such rules of procedure should be absorbed in the ETO as well so that the chances of confusion may be avoided among the judges as well as the lawyers.

Section 46-A discusses the integrity of the information system. The criteria for authentication of a document generated by an automated information

[16] For instance, if hash values are generated form a document then it is very easy to check whether the document ensures integrity or not. IT Act of India mentions hash values.

system is defined as "in working order". The meaning of working order is unexplained and remains ambiguous.

Pakistani law is also silent about the authentication of e-evidence through Metadata, hashtags or any other technology which are the most helpful tools for authentication of electronic evidence.

It was observed by in case *Arif Hashwani v. Sadruddin Hashwani* PLD 2007 Karachi 448, "…… that in my humble view audio, video-records cassettes CDs are admissible piece of evidence, however, the authenticity of same is always subject to proof in case the party against which it can be used disputed and or denied the authenticity and information contained in the said electronic documents".

Authentication in case of denial by the other party can be proved by providing audit trails of transmission and maintaining records of encryption.[17]

Problem of authentication of electronic evidence was highlighted by another Pakistani case *Qurban Ali v. State* 2007 PCRLJ 675 KARACHI-HIGHT-COURT-SINDH, where it was observed that

Anyone could send email to any other person, if he or she knew email account name of the other person… password of the receiving person was not required for that purpose. Address of the telephone holder/ owner, could be attained from PTCL/NTC. In that way email sending computer could be identified and the data of email could be retrieved form it by using computer Forensics Tools and it was also possible to prove it in court of law provided proper chain of custody was mentioned, it was, however, difficult to identify the particular person who sent the e-mail; that was the area where investigation by some police agency was required. No law existed by which cyber cafes were required to keep record of persons using the computer of cafes. Cyber, in circumstances did not keep record of persons using computers not did they keep history of data for long. Prosecution, in the case has not taken any effort to prove email in accordance with law which, in circumstances could not be relied upon and thus, were discarded.

Authentication by Applying Security Procedure

Qanun-e-Shahadat Order 1964 suggests that docuements must be authenticated by applying security procedure. It says;

[Explanation 4. Of Article 73 of Qanun-e-Shahadat Order 1984 states that

"- A printout or other form of reproduction of an electronic documents, other than a document mentioned in Explanation 3 above, first generated, sent received or stored in electronic form, shall be treated as primary evidence

[17]Encryption means translation of data into secret code. It is the most effective way to achieve security of the data. The reading of an encrypted file requires access to a password or secret key that enable to decrypt it.

where a **security procedure** was applied thereto at the time it was generated, sent, received or stored.]

Explanation 4 explains the criteria for accepting all copies as primary evidence. That is, the document must have been subjected to a security procedure before acceptance.

In physical documents, primary evidence is the original copy of the document. But the case is different in electronic evidence where all the documents produced through the automated system are primary. Such evidence fulfil the criteria of the original writing rule.

There was a case *Kashif Anwar vs. Agha Khan University,* 2013 YLR 2294 Karachi-High-Court-Sindh, the term security procedure was discussed and elaborated. The brief facts of the case are, that the appellant was a medical student of fourth year in Agha Khan University. One evening in September, 2002, plaintiff gathered with his friends to celebrate end examination party. During party, students used drugs. Unfortunately, one of the friend got fatal reaction to drugs and died the very next day. FIR was launched against the appellant. After the decision of disciplinary committee held within the university the student was rusticated from the university, for committing, abetting and keeping the possession of drugs in the vicinity of university.

The decision was reinforced by the court against which the appeal was filed. It was argued that the plaintiff did not get a chance to defend himself and that the rustication orders were unjust. As a result 3 audio tapes were submitted in court by defendant. Appellant challenged the authenticity of audio tapes. In this case Supreme Court observed that the audio tapes were inadmissible because there was lack of application of any security procedure to them for protection against tampering in terms of Art. 78 A of the Qanūn-e-Shahādat, 1984, which says that "if an electronic document is alleged to be signed or generated wholly or in part by any person, through the use of an information system, and such allegation is denied, the application of a security procedure for the electronic document has to be proved." This security procedure as prescribed by Sec 2 (x) of the Electronic Transaction Ordinance, 2002 states that; x) Security Procedure means a procedure which is

"(i) Agreed between parties;

i) Implemented in the normal course by a business and which is reasonably secure and reliable; or
ii) In relation to a certificate issued by a certification service provider, is specified in its certification practice statement; for establishing the authenticity or integrity, or both, of any electronic document which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices."

The court observed that in the present case, sub clause 1 was applicable since plaintiff had denied the authenticity of the tape-recording of his statement. It was imperative for AKU to have shown application of the above security procedure to the tapes prior to admitting them into evidence. But AKU failed to comply with this condition. Even AKU could not succeed in breaking the security tabs to prevent eraser, or re-recording, which is a very basic precaution that can be taken to prevent any tampering. Court observed that circumstantial evidence shows that the chain of custody of those audio tapes was not proved well.

For all the methods of authentication mentioned above and application of security procedure expert testimony has prime importance. Security procedure discussed above in section 2 (x) of Electronic Transaction Ordinance 2002. It is also discusses certificate issued by a certification service provider.

Section 2(i) of Electronic Transaction Ordinance 2002 defines term certification it states;

> (i) "certificate" means a certificate issued by a Certification Service Provider for the purpose of confirming the authenticity or integrity or both, of the information contained therein, of an electronic document or of an electronic signature in respect of which it is issued;

Certification services provider are the people who issues certificates and statement for establishing the authenticity, integrity or both of any electronic document which may require the use of algorithms or codes. Electronic Transaction Ordinance 2002, Section § 2(x).

The certificate providers are the experts in the field of IT, who must be capable of authenticating electronic documents are capable of conducting electronic discovery.

Authentication by Expert Testimony

Digital forensic expert opinion is becoming more common in cases of electronic discovery. They are called in electronic discovery cases for asking about how to use technology and giving low cost discovery methods.

It has always been discussed and debated that what should be the criteria of qualification of digital forensic expert? It is upon the discretion of the judge to decide whether an expert opinion is required in a particular case or not. The preliminary question to be decided, in cases of digital forensic expert is, whether the expert is competent or not? Although it is expressed by the court

that the judge should avoid unnecessary satellite litigation and exercise the discretion sparingly.

For acquiring expert's testimony, the judge has to keep in mind two aspects; whether or not the digital forensic expert carries any special qualification or experience regarding the subject matter, whether or not his opinion is acceptable due to some other incentive. An opinion acquired by the digital forensic expert, who does not have any special experience or knowledge is a question of weight, not admissibility.

Knowledge that is taken due to experience at work without special knowledge is acceptable too. For example, in the case of *R v Oakley* (2010) EWCA Crim. 2419, the opinion of a police officer was admitted regarding a road accident. The officer had 15 years' experience in the field of traffic division, who attended and passed a course as an accident investigator, and attended over 400 fatal road traffic accidents. But this rule does not apply everywhere, like, in *R v. Coultas*, [2002] WASCA 131, court rejected the forensic examination, of a mobile phone, by a police officer, without the relevant knowledge or expertise.

Since 1923, the role of experts in US legal system is based on Frye dictum. Frye v. United States, 54 App. D. C. 46, 293 F. 1013 (1923). According to this rule, it is the role of the judge to check whether a scientific position presented before the court is the accepted position of the relevant scientific community. In 1993, the Daubert precedent, 509 U. S. 579, 589, replaced the Fryer rule.

Daubert case was filed by two minor children and their parents (petitioners) against respondents that the serious birth defect of children was due to consumption of mother's prenatal ingestion of Bendectin, a prescription drug marketed by respondent. It was observed that condition of "general acceptance" is a necessary pre-requisite in a scientific case as prescribed by Fryer dictum. But following this rule rigidly may come out with odds with the rules meant to traditional barriers to "opinion testimony". It was observed by the court that "Frye made "general acceptance" exclusive test for admitting expert scientific testimony. The austere standard, absent from, and incompatible with, the Federal Rules of Evidence, should not be applied in federal trials". Thus the court should not only make sure that scientific testimony or evidence admitted is not only relevant, but reliable.
The court further observed that the expert must be proposing to testify to

1) Scientific knowledge that,
2) Will assist the trier of fact to understand or determine a fact in issue.

There are four questions to be answered in order to satisfy the above two question. The first one is whether that scientific knowledge can be tested. Second one is that whether the theory has been subject to peer review or publication. Third most important thing is that with respect to particular

scientific technique, court should know or check the rate of error. Fourth one is whether the theories are subject to standards governing their application. To check the standardization. These techniques are suggested by the court in order to prove the reliability of scientific knowledge.

In short, "General acceptance" rule by Frye Case was rejected to be a pre-condition to admissibility of scientific knowledge. Most important thing to be established is that expert testimony rests on a reliable foundation and is relevant to the issue.

The Daubert case based on cases of highly technical nature, which are grounded in science. But there are other cases which are applicable to skills. The question of applying Daubert case in non-scientific cases which are skill based was answered by Supreme Court in *Kumho Tire co. v. Carmichael court*, (97-1709) 526 U.S. 137 (1999) 131 F. 3 d 1433, Court extended Daubert approach to accessing the reliability of all expert opinions, whether the opinion is based on science, engineering principles or other "specialized knowledge". In practice the result is that every expert, including computer forensic expert shall be subjected to test of reliability. All opinions shall be scrutinized with respect to above four standards of testability, peer review, error rate, and standardization. It was further observed in *Kumho* case that the issues regarding the admissibility of digital forensic expert opinion are raised and solved by the judges on their own discretion in different circumstances. However, if the nature of the case requires expert testimony, then the experts should be objective, unbiased, reliable, and helpful to the court.

R v Stubbs [2006] EWCA Crim. 2312, is another important case on expert evidence for electronic data, which help defines the criteria of admissibility of digital forensic expert's opinion and how is it authenticated by other pieces of evidence? The appellant, in the said case, was convicted of being involved in the fraudulent money transfer from HSBC Bank of around 11.8 million Pounds. The fraudulent activities were carried out by using an online Banking System known as 'HEXAGON'. The appellant was a member of the Password Rest Team.

Prosecution called Mr. Richard Roddy for an expert opinion of HSBC, who was a worker at HSBC Bank. Although he was not the only digital forensic expert called by the court, the defense objected at trial to admissibility of Mr. Roddy's evidence on the ground that he lacked the expertise and independence to give expert opinion on the matters in question. It was accepted that his opinion is acceptable regarding the processes within HSBC and the ways in which the system was designed to operate. While his opinion about the detailed account of the actual activity within the system at the material times gave rise, was challenged. It was decided by the court that his opinion was admissible. Following test was applied in order the check the qualification of expert witness.

Court applied the test given in case, *R V Bonython*, (1984) 15 SASR 364, 366. There were two questions the court had to ponder.

(a) whether the subject matter of the opinion is such that a person without instruction or experience in the area of knowledge or human experience would be able to form a sound judgment on the matter without the assistance of witnesses possession special knowledge or experience in the area, and (b) whether the subject matter of the opinion forms part of a body of knowledge or experience which is sufficiently organized or recognized to be accepted as a reliable body of knowledge or experience, a special acquaintance with which by the witness would render his opinion of assistance to the court. The second question is whether the witness has acquired by study or experience sufficient knowledge of the subject to render his opinion of value in resolving the issues before the court. *R v Bonython*, [1984] SASR 45 at 46-47.

After reaching the decision to admit the evidence, the trial judge applied the above test. Court agreed that it was not disputed that the first question was resolved, because the Hexagon system was a subject for expert testimony, and the court went on to say about the second question, it is true that Mr. Rodd wasn't an IT specialist and his technical knowledge for such matters was limited but his knowledge, experience and skills made him qualify as an expert in this case.

The technical evidence offered by Mr. Roddy was not the only evidence of relevance that was submitted by the prosecution. There were other supporting evidences for the prosecution case. For example, the appellant left the building sometime after 5:00 pm and returned at 5: 27 pm. He claimed that he came back to collect his umbrella and that it had been raining, but the evidence from a CCTV located outside an office a few minutes away from the entrance showed that it's a bright sunny day at that particular time. The appellant could not produce the relevant paperwork authorizing him to change passwords. He lied during his internal interviews, and the evidence he gave to the police during questioning was also inconsistent. Stephen, (2012)

Journey of electronic evidence starts from electronic discovery, and go through the crucial stages of authentication. The last stage is expert testimony where digital forensic expert assist the court to judge whether the evidence is admissible, authentic and helpful or not. The most important stages during admissibility are authentication and expert testimony. A lot of work has been done on the above two areas in west. Pakistani law is also partly addressing these issues. However, the rules regarding authentication and expert testimony must be more clarifying and elaborative. Authentication techniques for electronic evidence need to be addressed in laws as well as

case law of Pakistan. Role of experts in Pakistani context need to be properly acknowledged in QSO as well as Judgments.

Expert Testimony in Pakistani Law

Qanun-e-Shahadat Order 1984 expressly provides that expert testimony can be acquired in case of electronic evidence in article 59. It states;

> **59. Opinions of experts:** When the Court has to form an opinion upon a point of foreign law, or of science/or art, or as to identity Of hand-writing or finger impressions, [or as to authenticity and integrity of electronic documents made by or through an information system shall be inserted; and] the opinions upon that point of **persons specially skilled** in such foreign law science or art, or in questions as to identity of hand-writing or finger impressions are [or, as to the function specification, programming and operation of information system are relevant facts.]Such persons are called experts.

Article 60 states further;

> **60. Facts bearing upon opinions of experts:** Facts not otherwise relevant, are relevant if they support or are inconsistent with the opinions of experts, when such opinion are relevant."

There are different views of judges regarding admissibility of expert testimony. For instance, in the case of *Fida Muhammad and another v. Umar Khattab,* 2013 CL C 1171 [Peshawar], it was observed by the court that expert testimony is a circumstantial evidence in nature. Circumstantial evidence, is weak evidence in absence of direct evidence, unless corroborated by other strong evidence. If the expert is not cross-examined in court it loses its credibility. On the same grounds expert testimony were rejected. Like, *"Allah Dino and two others case"* 1974 SCMR 311, an expert report which was not examined by the court was rendered inadmissible by the Honourable Supreme Court.

These types of rejections and low trust of courts on expert testimony can be observed when, court is not satisfied by the qualification of experts, which is mentioned as special skill in section 59 of QSO 1984. In case qualification of experts are fulfilled, their statements become strong proof. For instance, in case *Abdul Ahad v. The State,* PLD 2007 Peshawar 83, it was observed that*;*

> The most essential requirement of the law is that an expert on the particular subject whether Science, Art or Law including Muḥammadan Law must be a master in the relevant field because of special duty, training, experience and extensive research work carried out. The opinion of such an expert alone would be relevant and admissible.

Specialized knowledge mentioned in article 59 of QSO 1984 is elaborated in the above judgment which further clarifies that mastery in relevant field can be due to special training, extensive research work, or special duty. It is the responsibility of judge to determine whether the expert has gone sufficient training or study or he has sufficient experience to be rendered an expert in the given specialized field. It is not necessary that specialized knowledge be obtained professionally. (Mason, 2017)

Digital Forensic expert[18] opinion must be completely or partly based on his or her expert knowledge. It means that the opinion cannot be given outside the area of expertise. Facts on which the expert opinion is based must be available to the court for scrutiny. It must be clearly established that the facts on which the expert opinion is based, has solid foundation for it and how does his or her field of knowledge applies to the facts? The reasoning of expert opinion must be exposed, so that it satisfies the court that the opinion is based on the application of relevant knowledge and it is capable of being tested like any other testimony. (Daniel & Daniel, 2012).

Digital Forensic experts qualify as experts in court, during trial their responsibility is to prove the chain of custody, conducting electronic discovery motions, assisting in trial preparation, issuing search warrant affidavits etc. Computer forensic experts need some special qualifications to conduct digital forensic these qualifications are discussed at length in the following topic.

Conclusion

Electronic Discovery of data consists of following essential steps; checking privacy concerns, dealing with management and cost issues. These problems and solutions are well discussed and elaborated in western laws. Pakistan on the other hand, is at initial stage, in discussing these issues. Laws of Pakistan does not discuss electronic discovery and other issues related to it, like, cost issues, data management and privacy problems. Western countries on the other hand have established their infrastructure and laws to deal with these matters. Pakistan should accelerate to do the same to avoid any harsh consequences. In the process of electronic discovery evidence need to be well managed and free of privileged communication. In the case of non-availability of data at the time of demand by the court, heavy sanctions can be imposed. Economical and cost effective discovery expeditions are need of the hour.

[18] Digital forensics or Computer forensics can be defined as "a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. It has expanded to cover investigation of all devices capable of storing digital data." Digital forensic experts are hired all over the globe. Their main function if acquisition of data, to do forensic data analysis, and data recovery from multiple media types. "Digital Forensics."

Authentication of electronic evidence is the most important step for admissibility of electronic evidence. It is widely being accepted by western and Pakistani courts that modern evidence is admissible subject to its integrity. There are a number of ways of authentication of electronic evidence. For instance, authentication by hash tags, meta data, circumstantial evidence, oral testimony and expert testimony. All these methods are connected to each other one way or the other. More than one ways can be used to authenticate evidence. For authentication purposes differentiation between electronically generated evidence and computer stored evidence is to be known by the lawyers to establish evidential foundation. For the earlier type system which generated the evidence must be reliable. For computer stored evidence, authentication can be made by either of the methods mentioned above.

Digital forensic experts also play a vital role in investing tampering or other errors in it. They plays a key role in authentication of electronic evidence. Principles regarding the qualification of digital forensic experts are well established in western world. Pakistan needs to adopt the changes in its legal system for amicable solutions to problems related to discovery and admissibility of electronic evidence.

Electronic Transaction Ordinance and Qanun-e-Shahadat order does not define any methods of authentication. It says the system which generated the evidence must be in "working order". It suggests security procedure must be applied in order to authenticate electronic evidence. Expert testimony for electronic evidence is admissible under section 59 of Qanun-e-Shahadat order. Other details related to qualification of experts must be decided by Pakistani law according to their own needs.

References

Cendrowski, J. P. (2014). *Cloud computing and Electronic Discovery.* New Jersey: John Wiley and Sons.

Choo, D. Q. K. (2016). Big Forensic Data Reduction: Digital Forensic Images and Electronic Evidence. *Cluster Computing, 19*(2), 723-740.

Conrad, J. G. (2010). E-Discovery revisited: the need for artificial intelligence beyond information retrieval. *Artificial Intelligence and Law*. *18*(4), 321-345.

Davidson, Alan. (2009). *The Law of Electronic Commerce. New Delhi, ND:* Cambridge University Press.

Duranti, L., Corinne and Anthony, S. (2010), Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", *Arhivaria, Vol.* 70, 95-124.

_____ (2012), Trust in Digital Records: An Increasingly Cloudy Legal Area. *Computer Law and Security Law Review*, Vol. 28, 527-542.

Goodison Sean E., R. C. (2015). Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *RAND Cooperation*.

Haneef, S. (2006), Modern Means of Proof: Legal Basis for its Accommodation in Islamic Law, *Arab Law Quarterly* 20(4), 334-364.

Isom, K. (2006), Electronic Discovery Primer for Judges. *Fed. Cts. L. Rev.,*1(2), 25-40.

Robert, J. J. (2011). A Practitioner's Primer on Computer-Generated Evidence. *The University of Chicago Law Review, 41*(2), 254-280.

Judish, N. (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* New York: Office of Legal Education, Executive Office for United States Attorneys.

Daniel Larry., & Lars,. Daniel. (2012). *Digital Forensics for Legal Professionals: Understanding Digital Evidence from Warrant to Court room.* Waltham: Elsevier.

Long, R. M. (1986). The Discovery and Use of Computerized information: An Examination of Current Approaches. *Pepp L. Rev*, 1-22.

Martan Reidy, S. B. (2007). *Litigating with Electronically stored Information .* Norwood: Artech House.

Mason, S., & Seng, D. (2017). *Electronic evidence*. London; University of London Press.

Mason, S. (2014). Electronic Evidence: Dealing with encrypted data and understanding software, logic and proof. *ERA forum*, 25-36.

Meshal, R. (2014.). *Sharia and the Making of the Modern Egyptian: Islamic Law and Custom in the Courts of Ottoman.* Cairo: Oxford University Press.

Redish H, M. (2001). Discovery and the Litigation Matrix. *Duke Law Journal*, 561-628.

Rice, P. (2005). *Electronic Evidence: Law and Practice.* New York: ABA Publishing.

Roland, C. G. (2007). Hot issues in electronic discovery: information retention programs and preservation. *Tort Trial & Insurance Practice Law Journal*, 23.

Rothstein, B. J. (2007). *Managing Discovery of Electronic Information: A pocket Guide for Judges.* Federal Judicial Center.

Swift, E. (1987). Abolishing the Hearsay Rule. *Cal. L. Rev.*, 75, 495-520.

Wakin, J. (1972). *The Function of documents in Islamic Law.* New York: State University of New York Press.

Walsh, Decklan. "*Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions.*" *The New York Times,* 17 May. 2015, https://www.nytimes.com/2015/05/18/world/asia/fake-diplomas-real-cash-pakistani-company-axact-reaps-millions-columbiana-barkley.html Accessed 22 July 2019