ADMISSIBILITY OF COMPUTER EVIDENCE IN ISLAMIC LAW AND COMMON LAW: A PRELIMINARY ANALYSIS

HAFSA ABBASI*
DR. HAFIZ ANWAR**
*Faculty member
Department of Law,
Allama Iqbal Open University Islamabad, Pakistan
e-mail: haf.abbasi@gmail.com
**Professor of *Sharī'ah*,
International Islamic University Islamabad, Pakistan

Computer technology and its various applications have come to pervade all walks of life — be it social media, economy, higher studies, e-commerce etc., Common law principles on computer evidence are going through rapid change due to change in technologies and increasing use of electronic evidence in court. Islamic law also lays down very strong evidential principles for electronic evidence. Electronic evidence is treated as documentary and circumstantial evidence. In both the cases (when it is documentary or circumstantial evidence), it is admissible in civil cases. But its use is limited in criminal cases. That is, *Ḥudūd* and *Qiṣāṣ* cases cannot be decided solely on the basis of electronic evidence, unless corroborated by other evidences. Islamic law does not provide rules for electronic evidence, but it does provide important general principles, that can be used to test the standards advocated by modern law. The present research shall explore the principles of Islamic law for electronic evidence in the areas of documentary (*al-Kitābah)* and circumstantial evidence (*Qarīnah).* Then *Kitābah* or *Qarīnah,* are discussed to ascertain standards of *Sharī'ah* in civil and criminal cases.

Key words: *Documentary evidence, circumstantial evidence, electronic evidence, expert testimony, Islamic law*

Introduction

Imagine a person wakes up early in the morning and he is informed

that smart technologies and Internet has ceased to work in his country, for a few days. What would his life be like? No cell phone, no Internet, no laptops, no computers, no smartphones, no social media. This kind of life is unimaginable in this age. Imagine the loss that his business would have to bear? Or if he is an employee his institution would be at huge loss. Ultimately the economy of that state would be facing huge shocks.

The significance of computer, Internet and smart technologies is far beyond our imaginations. This is the factor that has helped man reshape it rules and govern it as smoothly as possible. How is it possible that something which is so important for mankind is not being paid any attention from the point of view of Islamic Law? It is right time to identify rules of Islamic law of evidence, dealing with computer and digital evidence.

Islamic jurisprudence provides for well-structured principles of law of evidence. These principles are general in nature. Which are applicable to upcoming new situations. There is no denying the fact that Islamic law does not provide specific rules for electronic evidence. However, it does provide important 'general principles' that can be used to test the standards set by modern law with a view to ascertain their compatibility with Islamic Law. These general principles can be derived from the areas of documentary (*al-Kitābah)* and circumstantial evidence (*Qarīnah)*, in Islamic law.

Present research, first defines electronic evidence and discusses its types. Then its significance is deliberated. It further covers stance of common law on electronic evidence, followed by how does it operate in civil and criminal cases. Then legal basis for admissibility of electronic evidence is discussed and rules of documentary (*al-Kitābah)* and circumstantial evidence (*Qarīnah)* are discussed one after the other, followed by *Qāḍī's* approach to both in case civil and criminal trials.

Definition and types of Electronic Evidence

Electronic evidence is defined as, "Information of probative value stored or transmitted in binary form"[1]. While binary represents the eventual storage format of all kinds of digital information, the term digital covers a broad range of data. So electronic evidence can appropriately be defined as "data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account

of either party more probable or less probable than it would be without the evidence."[2]

So, the definition of electronic evidence covers three aspects of information;

1. It includes all the evidence stored, created, altered in a computer
2. The computer devices include PCs, networks, phone systems, wireless devices, computer systems, smart cards, navigation systems, etc.
3. It includes only the data that is "relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes."[3]

National institute of Justice defined digital evidence as any information present in binary form and is reliable in courts. It is something which is present on a hard drive, a cell phone, laptop, flash card in a camera. Electronic evidence is usually linked to electronic crimes, similar to frauds relating to credit cards, or pornography. But electronic evidence is used to solve all types of cases. For instance, a mobile phone call record or an email address may reveal malicious intention of a suspect and his relationship with other criminals.[4] Digital evidence includes any information, or data sent or received by an electronic device, which can be utilized during investigation.

Mason categorises computer evidence on the basis of human input used in them. These are:

Computer Generated Data

This type of evidence is a document generated by computer and it does not involve human intervention. Examples of these types of record are data logs, telephone connections, and ATM transactions. The main evidential problem with this type of records is to establish that the computer program was working properly at that time. So here the testimony is not usually required as long as the system that generated the document is reliable.[5]

Computer Stored Data

It includes, the record of activities that involve the written content by one or more people. For example, emails, word processing files and

messages. From the evidential point of view, it would be necessary to establish that the content of the document is a reliable record of human statement. Here the witness who created the document must testify about the reliability. Otherwise, it can come under hearsay, which will make it inadmissible in court.[6]

Computer Stored and Generated Data

Record consisting of a mix of both human input and calculations generated and stored by a computer. Example of this type may be a spreadsheet that contain human statements (input to the spreadsheet program), and computer processing (mathematical calculations performed by the spreadsheet program). The evidential issue here would be to assess the document creation process. It means, to check how much of it is created by a human and how much of it is created by computer. It may be possible that human input could be hearsay, or the authenticity of the computer processing might be an issue.[7] Both issues shall be resolved accordingly.

The above-mentioned classifications are explained in the case of Elf Caledonia Ltd v London Bridge Engineering Ltd.[8] As it was rightly pointed out by the judge in the above case law that it is not always possible for the person who fed the data in computer to come and testify. So, there are some limits of such testimonies as well.

Significance of Electronic Evidence

Electronic evidence is the most important aspect of a crime and investigation. In fact, in the present times, it is very difficult to catch a criminal without any electronic evidence. There are many cases that support to this argument. One such case that shows the significance of electronic evidence is discussed below. In the case, the law enforcement agencies failed to solve the criminal case as there was no data in the modern gadgets to prove or disprove the facts.

Philip Welsh was a taxicab dispatcher who worked in Maryland. On February 2014, he was murdered at his home. At his workplace, he used technology and computers daily but at home, he never used such devices. He relied on landlines, hand written letters and typewriters. Friends and family often prompted him to try a device or the Internet, but Welsh never did. When he was absent from work, it was later found

that he had been murdered. He lived alone and had no enemies. In fact, he was a loveable person. His home was open to taxi drivers, who needed a place to sleep between shifts. Lack of digital evidence turned out to be a big hurdle in investigating the crime. Police had no way to find out what Welsh's activities were or whom he met. Without evidence such as text messages, emails, and web history, it was not possible to investigate. The murder of Philip Welsh remained unsolved and officers concluded that this happened due to the lack of digital evidence.[9]

Electronic Evidence in Common Law

Common Law now relies heavily on electronic evidence. When a suspect is caught, the Investigation Officer gathers proofs from him. The main information sources that help assess any link to the crime are the mobile phones which may contain call records, text messages, Internet browsing history, etc.[10]

It was observed by one of the US court in *Riley v California* that, *"*Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life".[11] It was also observed that the modern cell phones are not only phones but mini-computers in the hands of public, containing personal messages, social media posts, call records, browser history, contacts, things to do lists, personal notes, etc. All these activities' data play a vital role in connecting the dots of crime and chasing criminals. Mobile phones serve as a tracking system for the criminals.

Electronic evidence is almost unanimously accepted as a documentary evidence, real evidence and circumstantial evidence worldwide.[12] It is admissible as a documentary evidence in the case where body or text of document is sought to be proved. It is acceptable as a real evidence where content of document is not an issue, but availability of electronic evidence in accused's possession. For instance, presence of incriminating images or information in accused's computer or phone.[13] It is accepted as a circumstantial evidence when the case is to be proved through the circumstances. In *Public Prosecutor v. Neo Khoon Sing,* accused worked at National Environment Agency North-East Regional Office. He sent three emails containing false terrorist attacks warnings, from his official computer, hacking websites of ministry of home affairs and Prime Minister's office. Police found out the actual location from where the emails originated. Accused claimed defence of

alibi. But circumstantial evidence showed that the official computer was used for these emails. He claimed that an imposter accessed his computer and did this. But computer evidence showed that some time after these threatening emails, official email was sent.[14] So, this case like many others was solved on the basis of circumstantial evidence.

Modern means no doubt are of a great assistance to the law enforcement agencies but this technology is also being misused or abused. Technology is helpful to the criminals as well. Fragile nature of electronic evidence makes it prone to tampering, manipulation and destruction. The Common Law has tried to look into these problems. It is accepted worldwide that any evidence shall not be rejected solely on the ground that it belongs to modern technology. Different forms of latest evidences are increasingly being used in courts. During trials, judges are mostly asked to make rules for admissibility digital evidence. The decision on admissibility impacts the final result of the case, whether it be a civil or a criminal case.[15] Courts keep on trying to grapple with rules of evidence to deal with this area. The ease in which these kinds of evidence can be fabricated brings hurdles in the way of admissibility. Different kinds of evidence such as DVD, hard drives, SMS/MMS, chats, mails, and other kinds of computer generated evidence pose various problems and challenges for authentication.[16]

Generally four standards are applied for admissibility of electronic evidence:

1. The evidence must be relevant to facts in issue.
2. Evidence must be authenticated. This is the most important step of admissibility because it ensures complete trust or distrust of court on electronic evidence.[17] It deals with the challenges of authorship and alterations. Different techniques are applied for different kinds of electronic data, like, web content[18], e-mails,[19] business record and social media messages[20] etc. Following methods are usually used for authentication:

a) Authentication by testimony.[21]
b) Authentication by technical opinion (expert testimony).[22]
c) Authentication by Circumstantial Evidence.[23]
d) Authentication by other technical methods, like hashtags, meta data etc.[24]

The drilling process of authentication does not take place in each trial. It is only exercised where it is challenged by the opponent parties.

3. If the evidence in court's consideration is hearsay it is inadmissible.

This rule is generally applicable to computer stored evidence where data is manually fed.[25]

4. "Best Evidence Rule" which is derived from "Original Writing Rule", means that the evidence must be original, real, primary and direct. In electronic data it means that the copies produced through the mechanical process are exactly identical to the original. In Common Law printed duplicate copies are admissible as originals unless accuracy challenges are raised by the opponents.[26]

In Common Law electronic evidence is considered as reliable as physical evidence provided that the standards mentioned above are properly applied. In many European countries, three common situations are stated where electronic evidence is considered equivalent to traditional evidence. (1) The equivalence of paper documents with electronic document. In several legislations, the type of document is specified e.g. electronic receipts/contracts and notifications (fax) are compared with supporting paper receipts/contracts and notifications. (2) Similarity of electronic signatures with handwritten signatures. (3) The equivalence of electronic mail to postal mail.[27]

There is a group of European countries,[28] that assimilate electronic evidence with paper evidence. These countries give value to the electronic evidence as documentary evidence at trial.[29] This is the case commonly practiced in majority of the countries, including USA, UK, Pakistan.[30]

Electronic Evidence in Civil and Criminal Cases

Electronic evidence is treated differently in civil cases than in criminal cases because of the difference in their rules.[31] When electronic evidence is involved, one of the major differences between civil and criminal cases is, the chances of destruction of evidence. These chances are higher in civil cases because evidence is not usually seized, unlike criminal trials where the evidence is seized by the investigation officer.[32]

Electronic evidence has gained importance in most of the areas/ activities of daily life, such as modern economic transactions, commercial marketplaces and methods of commitment of crime, etc. That is why, electronic data has largely affected civil and criminal trials. In civil cases for example, there is an increased reliance on electronic communications, for solving a case. It is now a common practice, to request for discovery of several millions of pages or emails in civil disputes. Similarly, for investigation in criminal trials, reliance is increasing on social media sites,

such as Whatsapp, Skype, Facebook, etc, to gather evidence.[33] Response of legal profession towards electronic evidence in civil and criminal cases is in phase of fits and starts.

Electronic Evidence in Civil Trials

Rules of obtaining and storing evidence for civil trials are mostly governed by civil procedure codes of different countries. For instance, recent developments in new Federal Rules of Civil Procedure (FRCP) of USA and UK have tried to place to put some limitations on the kind of evidence that can be asked in electronic discovery, making the process less burdensome for both parties.[34]

Principles of electronic discovery for civil cases stipulate that parties are under obligation to disclose relevant evidence, which are demanded by the other party. Civil discovery means that parties have a right to request the court to compel the other party to hand over relevant evidences to them. Parties make a list of documents that are required by them. Other party upon request is bound to hand over, keeping the originals with them.

Methods of extracting evidence in civil discoveries are different from criminal investigation. Recently a model for e-discovery called e-discovery reference model (EDRM)[35], was published which included following steps.

i) Information Management.[36]
ii) Identification of evidence[37]
iii) Collection and preservation of evidence[38]
iv) Processing[39]
v) Reviews and analysis[40]
vi) Production[41]
vii) Presentation.[42]

In order to discuss working of electronic evidence in civil trials, a good example is UBS vs. Zubulake[43]. This was the case filed by Laura Zubulake, against her boss UBS Warburg, who promoted another person instead of Laura, despite the commitment made to her at the time of appointment, of a promotion at that particular time. Laura filed a case against gender discrimination at equal opportunity commission. The evidence of the case according to her were in emails exchanged between

UBS and Laura. Court ordered civil discovery of emails containing commitments made between plaintiff and defendant. Resultantly, the debate heated up between the parties and Laura demanded for more emails. The demand was refused by UBS on the grounds that searching for the requested pages would be cost prohibitive. Laura told the court that she presented almost 450 pages of emails in response to which only 100 pages were presented by UBS, which means rest of the emails were deliberately removed or deleted. Court asked UBS to explain the system of backing up of emails and data retention policies. After opinions were recorded by different experts, the court concluded that clearly the emails refused by UBS could be produced easily and that these emails were deliberately removed or deleted. The court resultantly decided to award 9.1 million to Zubulake as compensatory damages and 20.2 million dollars as punitive damages. Here it can be observed that proper management and archiving of electronic data is of immense importance in a civil trial. The reason is already mentioned above that in civil trials the evidence is the responsibility of the parties. In case of failure to produce required evidence, parties have to undergo heavy sanctions.

Electronic Evidence in Criminal Trials

In order to access the status of electronic evidence in criminal case, let us consider an example of a person Fred who steals money from a bank through fraudulent fund transfer. Fred uses a number of computers to hide his tracks. Let us assume that Fred uses a server run by a private university as his first intermediary and then a computer from public library. From his ISP he first hacks a university computer, with access to the university computer established, he hacks the library computer. From the library computer he finally attacks the main server of the bank. Fred is successful in guessing the password correctly. He creates a new account and instructs the computer that the account has $ 500,000 in it. He then transfers the money from new account to an account which is untraceable (offshore). The next day an officer from the bank finds out that money was transferred to a new account and is now missing. Bank calls the police.

The electronic crime scene looks very different. Apparently there is neither any eye witness nor any piece of real evidence. A digital detective (expert) would assess the situation and will find out the IP

(similar to a telephone number of Internet) address of the person who hacked the account. The bank's server kept a log of hacker's connection to the bank computer. The detective starting from IP address would follow the bread crumbs from the bank to appellant's computer. He would collect bits and bytes of electronic evidence in the system of bank and accused computer and assemble them in a way that identifies the plaintiff and proofs his guilt beyond reasonable doubt.

The first step would be to obtain stored record from the four computers used in the server attacks home computer, university, library and then bank computers. The procedure for collection of electronic evidence in criminal cases (such as hacking) involve three stages; collection of evidence, surveillance and the forensic investigation of suspect's computer.[44]

The key in most of the cases is to get access to the computer which was used to conduct this activity. If police gets an access to Fred's computer they would be able to get evidence of extra ordinary importance. It is possible for the detective to reconstruct details of what happened and when. Even the deleted files can be recovered.

Let us assume that the detective successfully extracts incriminating information from Fred's computer. Fred is found guilty and the matter goes to trial. Prosecution will present witnesses in a sequence of incidents. First a person from the bank will testify that money was stolen. Secondly, system administrators from intermediary banks will testify about the link in the chain of evidence. The system administrator of Fred's ISP will testify about the criminal activity that took place through the system. Finally, the government officials will testify that they found the computer from Fred's home. They will give any other circumstantial evidence which they found out from Fred's home such as, the user name and password of the bank written on a piece of paper, placed on the computer table. The government's case shall be proved beyond reasonable doubt that Fred committed the banking robbery.

Here in this case, the experts and the circumstantial evidence play a vital role, if the accused is interviewed and clues can be found from there. For instance, in another case, the accused stole fraudulently through a money transfer from the bank. The accused was a team member of password reset team. From among many other proofs against him, his lies during interview sessions and circumstantial evidence proved him guilty. He accessed the computer of office after his dismissal time from office. He came back to office 30 minutes after that. He was asked

about the reason of coming back, he said he came back to pick umbrella because it was raining. But the CCTV footage showed that it was a bright sunny day. Similarly, in case *US v. Siddiqui,* the accused denied of being the author of incriminating chats. But the investigation officers found out a name and address on a piece of a paper on his table, which was given in the chats.

In a nutshell, there are few things which are essential for a case of electronic evidence in criminal trials:

1. Oral testimony,
2. Expert testimony
3. Circumstantial evidence
4. Documentary evidence etc

Legal Basis for Admissibility in *Sharī'ah*

There is no doubt that any direct precedent for electronic evidence in the time of Prophet (ﷺ) and classical *fiqh* is not possible. But the saying of the Prophet "*bayyinah* is on claimant"[45] is broad enough to provide many things including modern means of proofs. Electronic evidence comes under two types of evidence and can be proven through them:

1. Documentary evidence *al-Kitābah,*
2. *Qarīnah*

Computer evidences and photographs are some strong analogous evidential foundations for electronic evidences.

Computer and Digital Evidence and Rule of *Al-Kitābah*

In the classical Islamic law, documentary evidence was named as *aurāq, hujjāj, sijīl, wathīqah, mukhadar*.[46] Documents in that time were physical only, such as written paper or parchment manuscripts. Such definition of jurists for documentary evidence was based on their observation and the need of time. But the most important thing for content of a document is that it can give information on it. So keeping in view the modern era and reliance of society on electronic documents,

Islamic scholars willingly expanded the definition of documentary evidence and added modern evidence into it.[47]

The Qur'ān gives a lot of importance to documentation. For instance, it orders to write down the transaction or any debt which is to be returned. It explicitly states in Surah al-Baqarah "O ye who believe! When ye deal with each other, in transactions involving future obligations in a fixed period of time, write them, let a scribe write down faithfully as between the parties."[48]

According to the above verse of the Qur'ān, a loan agreement signed by the debtor, will be a valid proof against his liability of payment. As electronic evidence is also a documentary evidence so this verse will also be applicable to electronic writings. For instance, Younus Sohaili, while writing about credit card transactions quotes above verse and analyses the concept of writing of a debt as below;

> "It is the opinion of the researcher that the credit card serves the purpose of writing the debt of the customer at the point of transaction. The card is swiped and the magnetic strip (or micro-chip depending on the design of the card) is read by the computer and the account of the customer is accessed via several levels of computer verification, afterwards the customer approves the amount of money that will be credited to his or her account and then the merchant will use the card reading machine to record or "write" that amount of debt onto the customer's account."[49]

Many narrations from the Prophet Muhammad (ﷺ) also established the precedent, regarding the orders about drafting legal documents and their enforceability in the court of law. For instance, Prophet (ﷺ) ordered his Companion 'Ali (R.A.) to draw up a document in his name at *Ḥudaībīyah*.[50] Another example is of Prophet Muhammad (ﷺ) commanded his representative to draft a written agreement when he purchased a slave from one of his Companions.[51]

Guiding principles given by the Qur'ān and *Sunnah* clearly established that documentary evidence had a significant role in agreements and commercial laws. This practice was unanimously endorsed by the Companions of Prophet (*Ijmā'*). Muslim jurists also agreed that documentary evidence is a valid means of proof in Islamic law.[52] But the most important element for admissibility of documentary evidence whether in Islamic law or computer evidence, is authentication.

Authentication of Documentary Evidence in Islamic Law

Acceptability of documentary evidence in Islamic law is not absolute. Allah, The Exalted, in His Book guides further about the criteria of admissibility. The Qur'ān explicitly states that "And bring to witness two just men from among you and establish the testimony".[53] After ordering to write down the debt, the same verse necessitates oral testimony of upright witnesses on transactions, in order to prove the authenticity and reliability in case of dispute. This does not mean that documentary evidence is inadmissible without oral testimony. This verse implies that there must be some surety which proves the authenticity of documentary evidence. As this practice is commonly used in Western law as well, where electronic evidence is authenticated by witnesses.[54] This happens in cases where there are doubts about the reliability of a document.

On the other hand, if the document is of such a nature that it is self-authenticating, then it does not need witnesses[55]. For instance, it was reported about Prophet (ﷺ) that he used to write letters and handed them over to his envoys who sent them forward without knowledge of its contents and the latter accepted them without asking for any verifications.[56] Judicial records of Ottoman Courts called *sijjīls,* are also a great proof to this argument. Such court records were mostly referred to without testimony for future reference. Majority of Muslim jurists accepted documentary evidence as valid means of proof in Islamic law.[57]

Islamic law primarily relied on oral testimony. But documentary evidence was not less important. For authentication of oral testimony, purgation was necessary. Condition of a specific number of witnesses for different wrongs, whether civil[58] or criminal[59] is also essential in the light of the Qur'ān and *Sunnah*.

Purgation is derived from an Arabic term *Tazkiyah*[60]. It is formal procedure which is carried out by the judge to check out the character of witnesses. The admissibility of statement of the witness depends on good reputation and his trustworthy behaviour. It shows a sense of responsibility of a witness regarding the degree of truth he is likely to speak during a trial. If his good deeds are dominating in his personality upon his bad deeds, he is able to testify. Islamic legal system puts great stress on purgation of witnesses. The reason is to get authentic evidence. According to Imām Sarakhsī, the statement of just and probable witness (*shāhid Ādil*) is how authentic oral testimony can be acquired.[61] Similarly, documentary evidence is either authenticated by just witnesses or other

sources which can prove of being trust worthy, such as public records, judicial registers, sealed documents, etc. So, it can be observed that authentication of evidence, whether oral or documentary, has an important place in *Sharī'ah*.

Application of Islamic Principles of Documentary Evidence on Electronic Evidence in civil and criminal cases

As mentioned above, documentary evidence was unanimously accepted by the jurists. But the extent of its use depends on type of the trial, i.e. civil or criminal. In case of civil trials where the disputes related to money matters, a legal maxim in Islamic law is applicable which says; "writings in the form of entries in merchant books, deeds of will, diaries, loan transactions, etc., are like talking to one another".[62] According to most of the jurists, such entries are admissible if they are authenticated by handwriting and signature experts or witnesses. This above mentioned rule is similar to "the best evidence rule" in Common Law.[63]

Ibn Qayyim does not require authentication of documents that are exchanged on daily basis as a customary practice. For example, as a proof of writing alone, he states; "When the interlocutor says what do you say about a stray animal engraved in its thigh, charity or endowment or locked"? Is it appropriate for the judge to pass a judgment on the basis of such marks, the answer was yes. It is the opinion of Mālikī school of thought and opined that such marks are stronger proofs than testimony. Ibn Qayyim also quoted Imam Ahmad who was once asked about the execution of deed of will found under the pillow of deceased person and there is no one to testify about it. He replied "yes if the handwriting of deceased was known for its uniqueness".[64]

So if this situation is applied in civil cases, indeed electronic evidence is a very strong mean of proof, if it passes the tests of admissibility. The aim of both Islamic law and Common Law is to seek evidence that is free of errors and tampering. In this situation, if the system that generates the electronic evidence is reliable, such evidence will be admissible without testimony. Based on the precedents of use of such reliable documents commonly in Islamic courts, the test for reliability of computer system is to be approved by an expert. But for business records the test is that the whole business is running on the basis of that data.[65]

Jurists agree upon the admissibility of electronic evidence in criminal cases that has *ta'zīr* punishments, but their opinion is differed upon for

establishing fixed crimes like *ḥudūd* and *qiṣāṣ*.[66] For instance, if there are some emails found from a boss who has tried to sexually assault his subordinates, it can be proven for the crime of sexual harassment. But the same messages, if they contain conversation about fun they both had dating alone with each other cannot be proven for *ḥadd* or *zinā* punishment against both, according to the majority. The argument given by the scholars are:

1. A legal maxim based on narration of Prophet (ﷺ) that governs prosecution of *ḥudūd*; "Fixed punishments are nullified by doubts".[67]
2. "The great danger of its fabrication and concoction for false charges, by saying that the ominous fabrication of *Uthman's* signature via a letter led to his tragic assassination."[68]

There is a minority of group who believe that official letters can prove *ḥudūd* and *qiṣāṣ*. For examples Ibn Qayyim is of the view that Imam Bukhari believed that one letter of the ruler to the other is admissible documentary evidence for crimes of homicide and *ḥudūd.* His opinion was based on example set by Prophet (ﷺ) when he wrote to Jews for the payment of *diyah* to the family of deceased person and another by Caliph 'Umar (R.A.) in *ḥudūd* punishments.[69] But obviously, this example cannot be applied to document mentioned above which is merely a private email, unless it is corroborated by confession of both the parties who committed *ḥudūd* offence.

It can be concluded here that application of electronic evidence in case of civil cases and *ta'zīr* crimes is agreed upon by jurists. But the same cannot be applied in case of *ḥudūd* and *qiṣāṣ*. Unless they are corroborated by other stronger pieces of evidence, such as oral testimony that are stipulated in *Qur'ān* and confession of parties during cross-examination.

But the importance of electronic evidence in today's world cannot be denied because most of the criminals are caught on the basis of CCTV films, video, recordings, pictures, call records, etc. These evidences are very strong in nature. These are the proofs and if authenticated properly cannot be negated by the accused. So there is a possibility that the guilty party is made to confess the crime during cross-examination or interviews. Otherwise, *ḥudūd* and *qiṣāṣ* on the basis of electronic evidence alone cannot be executed. In that case, judge has very vast powers under *ta'zīr* punishments. In order to keep the peace and harmony of society, such criminals must be given deterrent punishments.[70]

Computer Evidence and its Connection with Circumstantial Evidence

There are two ways in which circumstantial evidence can be connected to electronic evidence. These two ways are illustrated with the help of two case studies to have a better understanding of the concept.

1. Electronic crime is proved with the help of physical circumstantial evidence. A case *U.S v. Simpsons*,[71] illustrates it better. When the defendant objected that the conversation alleged to be between him and FBI agent, does not belong to him. The court rejected the plea and observed that government authenticated the chat room printouts by a number of circumstantial evidences. For instance, during the discussion in the chat room, the defendant gave the name, street number and email address. Later, during search of defendant's house, a page was found near his computer containing the email address, street number and telephone number given to the agent.

2. Electronic Evidence is circumstantial evidence itself. Physical crime is proved with the help of circumstantial evidence which is electronic in nature. This can be best illustrated by a case, in year 2012, when a person named, Christian Aguilar disappeared. He was a friend of Pedro Bravo and both studied at the same University at Florida. Three weeks later, the dead body of Augilar, was found from a grave, 60 miles away from his residence. He was last seen with his friend Bravo. Police suspected Bravo had some relation with the disappearance. After search it was found that he was in possession of Augilar's backpack. The reason why Bravo was upset with Aguilar was that he had started a relationship with Bravo's ex-girlfriend. Hence, digital evidence made this circumstantial case far more certain. Electronic evidence experts had access to Bravo's cell phone and got many key pieces of proofs. Examiners found out that in the cache for the phone's Facebook app, there was a screenshot of a Siri search made near the time of Aguilar's disappearance that read, "I need to hide my roommate." Determining the tower that received signals from the cell phone, showed that Bravo had moved far to the west after the disappearance. In the end, examiners were able to investigate that the flashlight app on the cell phone was used for almost one hour after the disappearance. After these evidences and proofs, Bravo was tried in the court, in August 2014. During cross

examination he admitted the crime and was convicted of first-degree murder.[72]

In both the above mentioned situations, either of the party who has successfully established strong relationship between authentic electronic and circumstantial evidence, has got great chances to win the case. The matters in which electronic evidence is the proof itself, as a circumstantial evidence to the case, it is considered as a very strong proof. These proofs are a centre of attraction for the investigation officers because these proofs cannot be denied. For instance, DNA test, finger prints, call records, text messages (record of the numbers and timings and on which texts are sent).

Qarīnah **in Islamic Law and Rules for Computer Evidence**

Circumstantial Evidence in Islamic Law is lexically derived from the word *Qarīnah*. The word *Qarīnah* (pl. *qarā'in*) implies association, linkage, affiliation or genuine evidence. In the juristic sense, *Qarīnah* implies logical inference derived from certain facts from which a distinct conclusion can be reached at.[73]

Technically, the meaning of *Qarīnah* in Islamic Jurisprudence is "some set of information or facts which demonstrate the presence or non-presence of a thing (fact). The evidence of fact must likely be proved in the court."[74] Or it denotes "any signs and indications which show the existence or non-existence of a fact in issue (the thing claimed)".[75]

Proving or disproving a fact with the help of *Qarīnah* is endorsed by the Qur'ān, *Sunnah*, and precedent of Companions of Prophet. The evidence in the Qur'ān includes:

> "So they both raced each other to the door, and she tore his shirt form the back. They both found her lord near the door. She said: "What is the (fitting) punishment for one who formed an evil design against your wife, but prison or a grievous chastisement? He said: "It was she that sought to seduce me from my (true) self" And one of her house hold saw (this) and bore witness, (thus) "If it be that his shirt is torn from the front, then her tale is true and he is a liar. But if it be that his shirt is torn from the back then she is the liar, and he is telling the truth!" So when he saw his shirt that it was torn at the back, (Her husband) said: "Behold! It is a snare of you

> women. Truly, mighty is your snare!" O Yūsuf, pass this over! (O wife), ask forgiveness for your sin, for truly you are at a fault."[76]

These verses relate the tale of Prophet Yūsuf (Joseph) in the Qur'ān and they are frequently cited in the *fiqh* books to legitimize the utilization of fortuitous proof in Islamic Law. The charge of enticement against the youthful Yūsuf was ruled outthrough circumstantial evidence alone.

Ibn Qayyīm was among the advocates of the utilization of *Qarīnah.* Indeed, even in *Ḥudūd* cases he stated that, "Whosoever refuses to apply *al-'Amarāt* and *al-'Alamāt* (*Qarīnah*) in Islamic Law, verily, he has destroyed many rules and had neglected many rights."[77]

Most of the authorities, especially contemporary legal scholars, treat forensic evidence as a form of *Qarīnah* (circumstantial evidence). For instance, Al-Zuḥaīylī maintains:

> "As a matter of fact in our contemporary time, there have emerged a number of powerful and clear forms of circumstantial evidences and indicators in the field of proof and evidence. For example, the identification of the culprit through fingerprints, blood testing, photographs, sound recordings, and blood sampling. . . . But the court has to be extremely cautious about using them as the chances of tampering with them are greatly worrisome."[78]

Prof. Anwārullah, another contemporary thinker, classifies a number of forensic processes as circumstantial evidence. These include, autopsy results on the corpse, blood spots, finger impression, footprints, identification by tracks, handwriting samples, injury marks, violence marks on private parts of body of victim, and presence of incriminating objects, such as the weapon of the offence, and tire and radiator marks on the body of victim in case of accident.[79]

Another renowned expert in this field, Dābur, includes forensic evidence as *al-Qarā'in al-Mustaḥdathah* (the modern types of circumstantial evidences). He points out that in case of an autopsy for determining the cause of death (for instance, when the criminal strangled the deceased and hanged him, just to show that the victim has committed suicide). Other examples include blood tests for identification purposes or verification of finger impression and foot-prints, found on the objects used in the killing. All the above mentioned techniques, according to him, are tools which make the case stronger and a best source of

authentication.[80] But this opinion is of a minority of jurists who are very few in number. Majority of the jurists think that *Ḥudūd* and *qiṣāṣ* cannot be executed on the basis of circumstantial evidence only without other corroborating evidences. But the judges have vast powers under the area of *ta'zīr* punishments. If they are sure that wrong is being done by the accused they can give strict punishments. There are jurists who think that judge can even give death punishment by way of *ta'zīr*.

Ibn Taīmīyyah, Ibn Qayyīm al-Jawzīyyah and Ibn Farḥun integrated circumstantial evidence into *fiqh* doctrine of evidence and procedure. Ibn Qayyīm went so far as stating that physical indicators are stronger evidence than the testimony of witnesses, because they do not lie. Expert witnesses, by knowing how to interpret physical indicators, or how to interpret "the language of things," become indispensable aids to judges.[81]

Conclusion

Classical Islamic Law did not leave any direct precedent for electronic evidence. But it did leave general principles given in *Sharī'ah* for evidence, which can help address new problems. Rules pertaining to documentary evidence and circumstantial evidence provide a very strong analogical base for electronic evidence. These *Sharī'ah* principles can be easily compared with Common Law rules on electronic evidence to check their permissibility under *Sharī'ah.*

Computer evidence is a very vast field carrying a large number of types in it. Significance of electronic evidence and its role in society is undeniable. It has put a great impact on trials and evidence system. Most of the cases involve electronic evidence, whether it be documentary evidence generated electronically from a bankor a circumstantial evidence, derived from a cell phone of accused, or from Internet browser history of accused. That is why judges are grappling with these issues and trying to settle the principles to have smooth working of electronic evidence during trial.

Four steps for seeking admissibility of electronic evidence are must. Among them are relevance, authentication, rule against hearsay and best evidence rule. All these rules are designed to overcome the doubts attached to electronic evidence. Fragile nature of electronic evidence leads to doubts about tampering, authorship etc. That is why authentication of evidence is of utmost importance. Different kinds of evidence need different methods of authentication.

Electronic evidence operates differently in civil and criminal cases.

In civil cases, electronic discovery is the most daunting task. Similarly in criminal cases, evidence is seized by the investigation officers. The method of investigating, extracting, and presenting electronic evidence in court is very different from traditional as well as civil evidence.

Legal basis for admissibility in *Sharī'ah* is based on rules of documentary and circumstantial evidence. The Qur'ān gives special importance to *Kitābah.* Same is the case with *Sunnah* of Prophet (ﷺ). During the glorious periods of Muslim empires like Abbasids, Ottomans, documentary evidence was heavily used in courts and was referred to as a strong mean of proof. Since electronic evidence is also a documentary evidence so it is admissible under Islamic Law. But Islamic Law admits authentic documentary evidence, either by testimony of just witnesses or documents which are self-authenticating (stamped, sealed), whose chain of custody is reliable and is free of doubts. Similarly, electronic evidence shall be duly authenticated by the technological means available for its authentication or by just witnesses or experts, as per Islamic Law. This case may be applied unconditionally in civil cases, but in criminal cases this rule does not apply in case of *Ḥudūd* and *qiṣāṣ.* These are fixed punishments, and cannot be executed solely on the basis of electronic evidence, due to element of doubt in it. If that element of doubt is erased by confession of parties, or oral testimony of just witnesses then *Ḥudūd* and *qiṣāṣ* can be executed.

There is no doubt that electronic evidence is a very strong circumstantial evidence, like, DNA, finger prints, pictures, videos etc. These pieces of evidence strengthen the case a lot, especially if these evidences are corroborated by other evidences, they erase the element of doubt in it. The rule of documentary evidence in case of *Ḥudūd* and *qiṣāṣ* applies to circumstantial evidence as well. But judges have very vast powers in case of *ta'zīr* punishments. Such offenders can be punished in a deterrent manner, to bring peace in society.

Notes and References

1 . Scientific Working Group on Imaging Technologies. (1999). Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System [on-line]. Forensic Science Communications, 1(3). Available: http://www.fbi.gov/hq/lab/fsc/ backissu/oct1999/swigit2.html.

2 . Dubey V (2017) Admissibility of Electronic Evidence: An Indian Perspective. Forensic Res Criminol Int J 4(2): 00109. DOI: 10.15406/frcij.2017.04.00109. https://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf

3. *Ibid*.
4. Office of Justice Program, National Institute of Justice, Digital Evidence and Forensics. https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx
5. Stephen Mason et al., *Electronic Evidence* 2nd edition (Haryana: LexisNexis, 2012)
6. *Ibid.*
7. *Ibid*.
8. *Elf Enterprise Caledonia Ltd v London Bridge Engineering Limited* [1997] ScotCS
9. Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, "Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence" Rand Cooperation, 2015, 3. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf. (Last Accessed, May 9, 2017) Also in, Dan Morse, Philip Welsh's simple life hampers search for his killer, Washington Post, May 6, 2014 https://www.washingtonpost.com/local/crime/philip-welshs-imple-life-hampers-search-for-his-killer/2014/05/05/1fd20a52-cff7-11e3-a6b1-45c4dffb85a6_story.html?utm_term=.cc88146e147f
10. For instance, a toddler died in the car by raising temperature. His father Harris was caught because he had searched in his chrome similar information, like, what temperature is required to kill a child in a vehicle. See, Michael Pearson, "Georgia toddler death: Who is Justin Ross Harris?" CNN News, June 28, 2014. http://edition.cnn.com/2014/06/26/justice/georgia-toddler-death-father/index.html. (Accessed January 30, 2017.
11. *Riley v California*, 573 U.S. __ (2014), p. 32.
12. Sayed Sikanadar Shah Haneef "Modern means of proof: Legal basis for its accommodation in Islamic law." *Arab Law Quarterly* 20, no. 4 (2006), p. 21.
13. *Ibid*.
14. *Public Prosecutor v. Neo Khoon Sing* [2008] SGDC 225.
15. Dubey V (2017) Admissibility of Electronic Evidence: An Indian Perspective. Forensic Res Criminol Int J 4(2): 00109. DOI: 10.15406/frcij.2017.04.00109 https://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf, p. 2.
16. *Ibid*.
17. *Lorraine v. Markel*. 241 F.R.D. 534 (D. Md. 2007), p. 14.
18. Lorraine v. Markel American Ins. Co. 241 F.R.D. 534 (D. Md. 2007), at 18.
19. *R v. Mawji (Rizwan)* [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct).
20. Ira P. Robbins, "Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence." *Minnesota journal of law, Science and Technology* 13, no. 1. (2013).
21. *States v. Kassimu* , 2006 WL 1880335 (5th Cir. Jul. 7, 2006)
22. *Frye v. United States,* 54 App. D. C. 46, 293 F. 1013 (1923), *Daubert v. Merrell Dow Pharmaceuticals*, Inc., 509 U. S. 579, 589
23. Orin S. Kerr, Computer Records and the Federal Rules of Evidence, (2001), US Department of Justice, 18.
24. Mason, *Electronic Evidence*, p. 254.
25. Susan E.E.B. Sherman, Hearsay and Evidence in the Computer Emergency Response Team (CERT), p. 5.
26. Paul Rice, *Electronic Evidence: Law and Practice,* New York, ABA Publishing, 2005, p. 190.

27. Insa, Fredesvinda. (2007), "The Admissibility of Electronic Evidence in Court (A.E.E.C): Fighting Against High-Tech Crime-Result of a European Study", *Journal of Digital Forensic Practice*, 1:4, 29. available at: http://dx.doi.ord/10.1080/15567280701418049.
28. Germany, Belgium, Spain, Finland, France, Ireland, Italy, Luxemburg, Portugal and Romania.
29. Fredesvinda, The Admissibility of Electronic Evidence, p. 29.
30. Qanun-e-Shahadat Order, 1984, art 2(x) and 164.
31. Larry Daniel and Lars Daniel, *Digital Forensics for legal professionals: Understanding digital evidence from warrant to court room* (Waltham: Elsvier, 2012), p. 113
32. *Ibid.*
33. Neutens, Tijs, Tim Schwanen, Frank Witlox, and Philippe De Maeyer. "My space or your space? Towards a measure of joint accessibility." *Computers, Environment and Urban Systems* 32, no. 5 (2008), p. 334.
34. *Ibid*.
35. Electronic discovery reference Model, edrm.net. Accessed January 30, 2017. https://pacc-ccap.ca/pacc/wp-content/uploads/2014/06/EDRM-Chart_v3.pdf.
36. It includes getting electronic house in order. If a litigation management and the digital investigator is organized and he has a sense of what is located and where is it located? Who has control over it? The task is going to be much more efficient. The particulars that we have been through in the last few pages which are required to conduct civil electronic discovery are particularly relevant here.
37. This process involves the location of potential ESI sources.The content and scope, breadth and depth of relevant materials are identied. In this phase the main task is to figure out what is needed? What hard copies are there what soft copies they are going to be useful? Who has access to the data? At this phase in house involvement is important.
38. This process may involve protection against destruction. Electronically stored information is preserved from a variety of sources (e.g., Tapes, PCs, networks, portable storage devices, etc.) and through a number of means. Investigators are not allowed to carry on the investigation process on the originals. So they preserve it and copy it on some other sources. In this process a digital investigator has to make sure that the data may not have any alteration or manipulation, otherwise the data will lose its integrity in the court.
39. It involves conversion and reduction of data. The data is transferred from original or intermediate media to uniform media on which analysis is to be performed.
40. In this phase relevance and privilege of data is evaluated. Hosting and searching
41. Consists of the generation and delivery of reports to varied recipients (e.g., firm associates, partnering law firms, corporate legal counsel or other service providers).
42. It means presentation in court.
43. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).
44. Orin S. Kerr, "Digital evidence and the new criminal procedure." *Colum. L. Rev.* 105 (2005), p. 285.
45. Prophet (ﷺ) said, "Evidence must be produced by the plaintiff and Oath must be made by the defendant" Kasani, vol. 7/287.

46. Muhammad Al-Zuhaily, *Wasail al-Ithbat fi al-Syariah al-Islamiyyah fi al-muamalat alMadaniyyah wa al-Ahwal al-Syakhsiyyah,* (Beirut: Maktabah al-Muayyad. 1994
47. Sa'di Mustapa, Mursilalaili, Abdul Rani Kamarudin, and Zulfakar Ramlee Saad. "Reception of electronic evidence from Islamic perspective." *Australian Journal of Basic and Applied Sciences* 9, no. 26 (sp) (2015), p. 31.
48. The Qur'ān [II:282], Translated by Yusuf Ali.
49. Ahmad Abdur-Raheem Sabree and Younes Souhaili, "Evidence in the Qur'ān Related to Credit Card Transactions." *Journal of Islamic Economics, Banking and Finance* 113, no. 3158 (2015), 7/
50. Muḥammad bin Isma'il (d. 256), *Saḥiḥ al-Bukhari*, vol. III, (al-Najat: dār al-Tauq, 2001), bab: Kaīfa Yaktub, tradition no. 2698.
51. Muḥammad bin Aḥmad bin abī Sahl shams al-' Āa'ema al- Sarakhsī, *Al- Mabsūt,* vol. XXX, Beirut, Dār al-Ma'rafa, 1993, p. 168.
52. Sikandar Shah Haneef, Modern means of proofs, p. 28.
53. The Qur'ān [LXV:2].
54. *States v. Kassimu* 2006 WL 1880335 (5th Cir. Jul. 7, 2006)
55. Jonathan Frieden, D., and Leigh M. Murray. "The admissibility of electronic evidence under the federal rules of evidence." *Richmond Journal of Law & Technology* 17, no. 2 (2011), p. 16.
56. Shams al-Dīn Abū Abd Allāh Muḥammad ibn Abū Bakr ibn Ayyūb al-Zurī l-Dimashqī Ḥanbalī Ibn Qayyim, al-Jaūzīah , *al-Turuq al-Hukmiyyah fi al-Siyasah al-Shar'iyyah*, Cairo, Dār ul-Madni, n.d, p. 220.
57. Abd al-Karim Zaydan, *Nazam al-Qada fi al-Shari'ah al-Islamiyyah*, Baghdad, Matba'at al-'Ani, 1984, p. 157.
58. In civil matters two witnesses are required in usual circumstances, for instance, child custody, marriage, contracts, wills, debts. Etc.
59. In criminal cases number of witnesses is different in different type of offences. For instance in case of slandering and adultery four just witnesses are required. Other hudood offences require two just witnesses.
60. Purification.
61. Muḥammad bin Aḥmad bin abī Sahl shams al-' Āa'ema al- Sarakhsī, *Al- Mabsūt,* vol. XVI, Beirut, Dār al-Ma'rafa, 1993), p. 112.
62. See articles, 1606 to 1612 of The Mejelle, Trans.Tyser. C. R, Lahore: Law Publication Ltd, 1980. See also Zaydan, *Nazam al-Qada fi al-Shari'ah al-Islamiyyah* 157.
63. Haneef, Modern Means of Proofs, p. 29.
64. *Al-Turuq al Ḥukmiyah*, p. 216.
65. Mason, *Electronic evidence*, p. 145.
66. Haneef, Modern Means of Proof, p. 362.
67. Muhamad Ibn 'Isa al-Tirmidhi, Sunan al-Tirmidhi, vol. IV, Beirut, al-Maktab al-Islami, 1988, p. 25.
68. Haneef, Modern Means of Proof, p. 363.
69. *Al-Turuq al Ḥukmiyah*, 218.
70. Ahmad Syukran Baharuddin et al., Fiqh Forensics: Integration between Sciences and Islamic Law for Autopsies and Identification of Deceased, *Sains Humanika* 4:2 (2015), p. 3.

71. 252 U.S. 465 (40 S.Ct. 364, 64 L.Ed. 665).
72. Sean E. Goodison, C. Davis. Robert, and A. Jackson. Brian. "Digital evidence and the US criminal justice system." 3. Also in Lauren Effron, Jim Dubreuil And Laura Ramirez "Girlfriend at Center of Gainesville Love Triangle Never Thought Killer Ex Was Capable of Murder " New York, ABC news, Aug 20, 2014.http://abcnews.go.com/US/girlfriend-center-gainesville-love-triangle-thought-killer-capable/story?id=25060406.
73. Lisān al-'Arab, s.v "Qarīnah", al-Misbāḥ,,al-Munīr, s.v "Qarīnah",
74. Muḥammad 'Amīm al-'Ihsān al-Mujaddī al-Barkatī, *Qawa'id al-Fiqh,* vol. I, Karachi, Sadaf Publishers, 1986, p. 428.
75. Milton J. Cowan, *Dictionary of modern written Arabic,* 3rd ed., Beirut, n.p., 1974, 760; Elias A. Elias, *Modern Dictionary: Arabic English*, Beirut, Dar al-Jalil, 1986), p. 537.
76. The Qur'ān [XII:25-29].
77. Muḥammad bin abī Bakr bin 'Ayūb ibn Qayīm al-Jaūziah, *Al-Turuq al-Ḥukmīyah* (Maktabah Dār al-Bayān, n.d), p. 4.
78. Wahbah al-Zuhaīlī*, "Al-Fiqh al-Islamī wa 'Adiltuhu",* vol. VI*, Damascus, Dār al-fikr, 1985, p. 556.*
79. Sikanadar Shah Ḥaneef, "Modern means of proof: Legal basis for its accommodation in Islamic law", p. 343.
80. *Ibid*, p. 345.
81. Ron Shaham, *The Expert Witness in Islamic Courts; Medicine and Crafts in the service of Law*, London, The University of Chicago Press, 2010, p. 38.

Bibliography

1. Alā*' al-Dīn* Abū Bakr bin Mas'ud bin 'Aḥmad al-Kāsānī, (d. 587H), *"Badā'i' al-Ṣanā'i fī tartīb al-sharā'i*". 2nd ed., vol. VII, Dār al-Kutub al-'Ilmīah, 1998.
2. Al-Nīsābūrī. Muslim bin al Ḥjāj Abū al-Ḥassan al-Qashīrī*, Saḥī,,Muslim.*, Beīrūt: dār 'Iḥyīā' al-'arabī. n.d).
3. Al-Jawziyyah, Ibn Qayyim, and Muhammad bin Abk Bakr. "A*l-Turuq al-Hukmiyyah fi al-Siyasah al-Shar'iyyah* (Cairo: Dār ul-Madni, n.d), (1953).
4. Al-Shaf'ī, Abū Ḥussain Yaḥyah bin'Abī al-Khaīr al-'Imranī "*Al- Bīyān fī-Mazhab Imām Shafaī*", vol. XIII, Jaddah, Dār al-Minhāj, 2000.
5. Al-Shīrāzī . Abū Yūsuf, "Al-*Muhazab fī al-Fīqh al-Imām Shaf'aī*", vol. III, Dār al-Kitab al-'Ilmiah, n.d.
6. Al-Qurtubī. Abū 'Umar Yūsuf bin 'Abdullah, "*Al-Kāfī fī Fiqh al-Madīnah*", vol. II, Riadh, Maktabah al-Riadh al-Ḥaditha: 1980.
7. Al-Damishqi. Abdul Mughnī bin Ṭalib bin Ḥamād bin 'Ibrahīm, "*Albāb fī Sharḥ,,al-Kitāb*", Beīrūt, Maktabah 'Ilmiah, n.d.
8. Al-Sarkhasī Shamsud-u-Dīn Muḥammad ibn Aḥmad ibn Abī Sahl, *al-Mabsūt,*, vol. XXX, Beirut, Al-Ma'rifah publishers, 1998.
9. Amnon. Cohen, the Guild of Ottomon Jerushelum. Boston: Brill, 2001.

10. Al-Zuhaīlī Wahbah*, "al-Fiqh al-Islamī wa 'Adiltuhu",* vol. X, .Damascus: Dār al-fikr, 1985.
11. Dabūr, Anwar Mahmud. A*l-Qara'in wa Dawruhafi al- Fiqh al-Jina'i al-Islami.* Cairo: Dar al-Thaqafah, al-Arabiyyah, 1985.
12. Seng, Daniel KB. "Computer Output as Evidence." *Singapore Journal of Legal Studies,* July 1997 (1997), pp. 159-166.
13. Duranti, Luciana. Rogers, Corinne. Sheppard, Anthony. "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", *Arhivaria*70 (Fall 2010); pp. 95-124.
14. Davidson, Alan. T*he Law of Electronic Commerce.* New Delhi: Cambridge University Press, 2009.
15. Daniel, Larry and Lars Daniel. *Digital Forensics for legal professionals: Understanding digital evidence from warrant to court room.* Waltham: Elsvier, 2012.
16. Leroux, Oliveier. "Legal Admissibility of electronic evidence," International Review of Law, Computers & Technology 18, no. 2: (2007), pp. 193-220.
17. Fredesvinda Insa (2007), "The Admissibility of Electronic Evidence in Court (A.E.E.C): Fighting Against High-Tech Crime-Result of a European Study", Journal of Digital Forensic Practice, 1:4, 285-289, accessed: May 9, 2017. http://dx.doi.ord/10.1080/1da5567280701418049
18. Finkelstein, Sheldon M., and Evelyn R. Storch. "Admissibility of Electronically Stored Information: It's Still the Same Old Story." *J. Am. Acad. Matrimonial Law.* 23 (2010), p. 45.
19. Goodison, Sean E., Robert C. Davis, and Brian A. Jackson. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. RAND Corporation, 2015. http://www.jstor.org/stable/10.7249/j.ctt15sk8v3.
20. Goodison, Sean E., Robert C. Davis and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *Santa Monica, CA: RAND Corporation*, 2015. http://www.rand.org/pubs/research_reports/RR890
21. Gauthier, Johanne. "The Admissibility of Computer-Generated Evidence: An Overview" *Canadian Maritime Law Associates*, November,1997. http://www.cmla.org/papers/Admissibility%20of%20Computer%20Generated%20Evidence.Johanne%20Gauthier. 28. Nov. 1997. pdf (Last Accessed January 23rd, 2017).
22. Haneef, Sayed Sikanadar Shah. "Modern means of proof: Legal basis for its accommodation in Islamic law." *Arab Law Quarterly* 20, no. 4 (2006), pp. 334-364.
23. Ibn Nujaīm. Zaīn al-Dīn bin Ibrahīm bin Muḥammad, "*al-Baḥr ar–Rā'iq Sharḥ Kanz al-Daqaiq*", vol. VIII, Dār al-Kitāb al-Islāmī, n.d.
24. Ibn Rushd. Abū al-walīd Muḥammad bin Aḥmad, "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid",* vol. IV, Cairo, Dār al-Ḥadith, 2004.
25. Ibn 'Ābidīn, Muḥammad Amīn bin 'Umar, *"Hāshiyah ibn 'Ābidīn: Rad al-Muḥtār 'Ala al-dār al Mukhtār*", vol. VI, Beīrut: Dār al-fikr, 1992.
26. Ibn Taimīah, Taqqi-u-din Muḥammad. (d. 728), *Majmī' Fatāwā Shaykh al-Islām*

Aḥmad B. Taimīah, vol. XXXV, Majma‘ al-Malik Fahad li-Tabā‘ah Muṣhaf, 1995.

27. Kerr, Orin S. “Digital evidence and the new criminal procedure.” *Colum. L. Rev.* 105 (2005), p. 279.
28. Duranti. Luciana, Rogers, Corinne, And Sheppard. Anthony, “Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later”, *Arhivaria*70 (Fall 2010); pp. 95-124.
29. _____ “Trust in digital records: An increasingly cloudy legal area”, *Computer Law and Security Law Review* 28, (2012): 527
30. Leroux, Olivier. “Legal admissibility of electronic evidence 1.” *International Review of Law, Computers & Technology* 18, No. 2 (2004), pp. 193-220.
31. Meshal, Reem A. *Sharia and the Making of the Modern Egyptian: Islamic Law and Custom in the Courts of Ottoman.* Cairo, Oxford University Press, 2014.
32. *Maūsūa Fiqhiyah al-Qūītīyah*, vol. XLV, Qūaīt: Dār al-Salāsil, 2006.
33. Mawsilee. Abdullaah al, *Al-Ikhtiyaar Li Ta’leel al-Mukhtaar*, ed. ‘Ali Abdul-Khayr and Muhammad Sulaymaan vol. I. Damascus: Dar al-Khayr Publishers, 1998.
34. Mason, Stephen. et al., *“Electronic Evidence”* 2nd edition. Haryana, LexisNexis, 2012.
35. _____”Electronic evidence: dealing with encrypted data and understanding software, logic and proof.” In *ERA Forum*, vol. XV, No. 1, pp. 25-36. Springer Berlin Heidelberg, 2014.
36. Posner, Richard A. “An economic approach to the law of evidence.” *Stanford Law Review* (1999), pp. 1477-1546.
37. Rice, Paul. P. *Electronic Evidence: law and Practice.* New York: ABA Publishing, 2005.
38. Robert, Jerome J. , “A practitioner’s primer on computer-generated evidence”, *The University of Chicago. Law Review* 41(2), pp. 254-280
39. Muḥammad bin Isma‘il (d. 256), *Saḥiḥ al-Bukhari*, vol. IX al-Najat: dār al-Tauq, 2001.
40. Swift, Eleanor. “Abolishing the Hearsay Rule.” *Cal. L. Rev.* 75 (1987), p. 495.
41. Turner, Philip. “Digital provenance – interpretation, verification and corroboration”, *Digital Investigation* 2.1 (2005), pp. 45-49.
42. U.S Government, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations*, (General Books, 2011), accessed: September 1, 2015. thttp://www.cybercrime.gov/s&smanual2002.htm, October 2004.
43. Wakin. Jeanette, *The Function of documents in Islamic Law*. New York, State University of New York press, 1972.