	Penerimaan Jawatankuasa Fatwa Negeri-Negeri Terhadap Keputusan Muzakarah Jawatankuasa Fatwa Majlis Kebangsaan Bagi Hal Ehwal Ugama Islam Malaysia Zulfaqar bin Mamat	
19	**The Authenticity Of Electronic Document Under Islamic Law And Malaysian Law Of Evidence** Mursilalaili binti Mustapa Sa'di and Abd. Rani bin Kamarudin	
20	**Pengurusan Waqaf Pendidikan di Malaysia Ke Arah Kemajuan Tamadun Ummah: Suatu Tinjauan Awal** Mashitah Sulaiman, Mohd Nazir Ahmad, Suhailiza Md Hamdani dan Anita Ismail	
21	**Amalan Pensijilan Halal Malaysia** Lokman Bin Ab.Rahman	
22	**Peranan Lagu Dalam Dakwah Di Kalangan Masyarakat Remaja** Kalsom Ali, Muhammad Nizar Mohd Sobri & Mohammad Nashief S. Disomimba	
23	**Kesan Penggunaan Video Pendek Sebagai Medium Dakwah Kepada Remaja** Kalsom Ali, Nor A'shikin Binti Abdul Halim & Mohammad Nashief S. Disomimba	
24	**Integrasi Naqli Dan Aqli Dalam Isu Etika Kaunseling** Majidah Mat Jusoh dan Haslee Sharil Lim Abdullah	
25	**Pengurusan dan Pentadbiran Organisasi di Institusi Hal Ehwal Islam di Malaysia** Khairunneezam Mohd Noor	
26	**Managers Perception On Organizational Management In Islamic Perspective: A Study In JAKIM** Nur Hanan Ab Aziz and Khairunneezam Mohd Noor	
27	**مفهوم الدين اليهودية ومقف الإسلام منها** محمد نصيف س. ديسوميمبا، عبد السلام س. دسوميمبا، أحمد نجا مختار، كلثم بنت على	

PROSIDING

SEMINAR KEBANGSAAN PENYELIDIKAN PENGURUSAN HAL EHWAL ISLAM DI MALAYSIA

FAKULTI KEPIMPINAN & PENGURUSAN

UNIVERSITI SAINS ISLAM MALAYSIA

11 OGOS 2020

EDITOR:

Khairunneezam Mohd Noor

Zulkiple Abdul Ghani

Suhailiza Mohd Hamdani

UNIVERSITI SAINS ISLAM MALAYSIA

جامعة العلوم الإسلامية الماليزية

ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

JAKIM

MAIWP

UNIVERSITI SAINS ISLAM MALAYSIA

SEMINAR KEBANGSAAN PENYELIDIKAN PENGURUSAN HAL EHWAL ISLAM MALAYSIA

Perpustakaan Negara Malaysia Data Pengkatalogan-dalam-Penerbitan

Seminar Kebangsaan Penyelidikan Pengurusan Hal Ehwal Islam
(2020 : Nilai, Negeri Sembilan)
PROSIDING SEMINAR KEBANGSAAN PENYELIDIKAN PENGURUSAN HAL EHWAL ISLAM DI MALAYSIA : FAKULTI KEPIMPINAN & PENGURUSAN UNIVERSITI SAINS ISLAM MALAYSIA 11 OGOS 2020 / EDITOR: Khairunneezam Mohd Noor, Zulkiple Abdul Ghani, Suhailiza Mohd Hamdani.
ISBN 978-967-440-870-1
1. Islam--Congresses.
2. Government publications--Malaysia.
I. Khairunneezam Mohd Noor. II. Zulkiple Abdul Ghani.
III. Suhailiza Mohd Hamdani. IV. Judul.
297

ISBN 978-967-440-870-1

THE AUTHENTICITY OF ELECTRONIC DOCUMENT UNDER ISLAMIC LAW AND MALAYSIAN LAW OF EVIDENCE

Mursilalaili binti Mustapa Sa'di[1] and Abd. Rani bin Kamarudin[2]

[1]Department of Federal Territory Islamic Affairs. laili.mustapa@jawi.gov.my

[2]International Islamic University Malaysia, Associate Professor: rani@iium.edu.my

ABSTRACT

With the advancement of technology, the ways human communicates and interacts with each other have changed exponentially, where face to face or physical meetings and contacts can now be replaced with google meet, emails, video conferencing, digital signature etc. in ensuring that the proposed or intended affairs are successfully done but is no less efficient, time and cost saving. As the conversation took place through digital platform, it is automatically recorded in binary format, and the electronic evidence is usually automatically generated, recorded and stored. As dispute sometimes could not be avoided, the parties involved could turn to this electronic document to prove their facts in addition to document in traditional format. The fact or facts contained in such document to be adduced in evidence must be legally relevant, primary evidence and authentic as required by the Malaysian Evidence Act 1950 (Act 56). Islamic Law of Evidence too requires the fact presented as evidence in the form of document has to be authentic. The truth of its contents is a separate matter that need to be proven. However, due the nature of electronic evidence being relatively fragile, easily altered and manipulated, countries like Canada, India, and Singapore, have adopted in their Evidence Act, authentication provisions which is unwittingly consistent with the principles of Islamic Law of Evidence. This research is a qualitative research which used data collection and data analysis including library research and semi-structured interview. The finding of this research established that both common law and Islamic law requires that to adduce a document, its authenticity is one of the conditions of admissibility. Countries following common law has even gone further to insert newer authentication provisions in their law of evidence to accommodate the reception of electronic evidence or computer-generated document driven by newer technology. It is proposed that the Malaysian Evidence Act 1950 continues to be updated to keep pace with electronic document or computer-generated document driven by newer technology. However, there must also be provisions to ensure that the authenticity of electronic document must be supported by evidence capable of supporting a finding that the electronic document is that which it is purported to be. This technology driven document is also known as digital document, electronic document or computer-generated document.

Keywords: Electronic evidence, authenticity.

1. INTRODUCTION

Documents are now no longer only on paper and ink but in discs, memory card in computers, smartphones etc. which can be easily shared with others in tangible and intangible form i.e. electronically. The use of electronic document is now so wide spread that laws are made to accommodate them to be adduced in evidence. Unfortunately, electronic evidence presents its own issues which are fragile[1], easily altered and manipulated[2], hence there is an authentication[3] issues. Apart from electronic evidence fragility, there is an issue of specials skills and knowledge in acquiring and authenticating electronic evidence[4] for the same to be admissible in court.

2. NATURE OF ELECTRONIC DOCUMENT

Electronic document is defined as any type of output in digital form[5] that have relation with electronic devices[6] i.e. audio recording, digital document or photograph, video conferencing[7], that is used and

---

[1] Brenner, Susan W, "Cybercrime Metrics: Old Wine, New Bottles?", *Virginia Journal of Law & Technology*, vol. 9, no 13, (2004): 11.

[2] Chaikin, David, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence", *Crime Law Soc. Change*, vol. 46, no. 4-5, (2007): 242; Thomson, Lucy L "Admissibility of Electronic Documentation as Evidence in U.S. Court", (2011), The Center for Research Libraries Human Rights Electronic Evidence Study", via Center for Research Library, <https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf.>.

[3] Newman, Zachary G. & Ellis, Anthony "The Reliability, Admissibility, and Power of Electronic Evidence", *Pretrial Practice & Discovery*, vol. 19, no. 1, (2010): 1.

[4] Whitcomb; Council of Europe Electronic Evidence Guide agrees that electronic evidence is similar to that of traditional, in term of accepting it in the court of law, where the party producing it must ensure it authenticity, because of electronic evidence fragility.

[5] Whitcomb, Carrie Morgan "A Historical Perspective of Digital Evidence: A Forensic Scientist's View", *International Journal of Digital Evidence*, vol. 1, no. 1, (2002); Mason, Stephen, *International Electronic Evid*ence. (London: British Institute of International Comparative Law, 2008), 25.

[6] P. Sathasivam. "Appreciation of Evidence Including Evidence Recorded through Electronic Media for Sessions Cases". Lecture delivered during Training Programmed for District Judges Under the aegis of 13th Finance Commission Grant at Tamil Nadu State Judicial Academy. (2011).

[6] Council of Europe Electronic Evidence Guide unpublished work.

[7] Mason, Stephen, *Electronic Evidence*, (Australia: LexisNexis Butterworth,2nd edn., 2011), 25.

relevant at trial[8]. Examples of electronic document are e-mail, digital photographs and audios, global positioning system (GPS) data, internet browser histories, computer memories and printout, cellular phone missed, dialled and received called histories and short messaging text. The earliest computer operated on a "batch" or "job" basis, where large amounts of data were processed and the reports were generated. There was no user interaction. The report-of transaction on an account, of the product of a database- were the only forms of evidence available[9].

Another term for electronic document is Electronically Stored Information (ESI)[10]. ESI includes emails, voicemails, instant messages, text messages, documents and spreadsheets, file fragments, digital images, and video. There has been a major shift from conventional media to electronic digital media. "It is estimated that ESI has become exponentially greater in volume than that of conventional media".

As technology advances, storing and retrieving information has become not only easy but also cheap, hence documents remain, by and large, paperless. Before this, document is traditionally done on paper. With the introduction of electronic devices, the definition of document has been widened to include electronic output. Electronic output is any data that are associated with electronic devices that is created, manipulated, stored, communicated or transmitted in digital form including output of analogue format such as video or audio[11]. Electronic document or output could be any information or data in electronic devices such as information databases, operating system, application program, electronic or voice mail message and record that it created or stored in it. From the literature, it could be understood that some writers when describing electronic document used term like IT evidence, digital evidence, computer

---

[8] Egohan, Casey, *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet*, (Amsterdam: Elsevier Academic Press. 2nd ed., 2004).
[9] Sommer, Peter, "Emerging Problems in Digital Evidence", *Criminal Justice Matters*, vol. 58, no. 1, (2004): 24.
[10] Gaetano Ferro, Marcus Lawson and Sarah Murray, "Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know", *Journal of the American Academy of Matrimonial Lawyers*, vol. 23, (2010): 1. For them ESI is "information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software."
[11] Mason, Stephen, 25.

evidence,[12] computer related evidence, computer generated evidence[13], web-based evidence[14] and electronic evidence. However, all of these terms are a subset of a general term that discusses evidence by electronic means namely electronic evidence.

Electronic document has a broader definition compared to other definition. It is because electronic document are all forms of data, including the output of analogue device, such as video and audio tape recording which is not originating from digital form and data in digital format[15]. Thus, electronic document could be defined as "a data (comprising the output of analogue device 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 a factual account of either party more probable or less probable than it would be without the evidence"[16]. Electronic evidence is document that was created in digital format with the advancement of technology apart from the physical form[17].

In Malaysia, there is no exact definition in any statute on the term "electronic evidence", "computer evidence" or "digital evidence", except the word 'electronic', "computer output", "evidence" and "document". Those words are defined in Electronic Commerce Act 2006 (ECA), Computer Crime Act 1997 (CCA) and Evidence Act 1950 (EA). ECA 2006 defined "electronic" as "the technology of utilizing electrical, optical, magnetic, electromagnetic, biometric, photonic or other similar technology"[18]. From this definition, it implies that electronic is a technology that utilized electric or magnetic to perform various functions which is related to the technology. It could be computer and other devices such as a smart phone.

---

[12] Chaikin, David, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence", *Crime, Law and Social Change*, vol. 46, (2007): 240. Springer Link, via Springer, <http://dx.doi.org/10.1007/s10611-007-9058-4>; Fahim Akhter, "E-Commerce Security: The Categorical Role of Computer Forensic Online Crime" in *Intelligence and Security Informatics: IEEE ISI 2008 International Workshops: PAISI, PACCF, and SOCO 2008 Proceedings,* Taipei, Taiwan, 17 June 2008), 300. ResearchGate, https://www.researchgate.net/publication/221246751_E-Commerce_Security_The_Categorical_Role_of_Computers_in_Forensic_Online_Crime. DOI: 10.1007/978-3-540-69304-8_30. (accessed 19 July, 2013).

[13] Duryana Mohamed and Zulfakar Ramlee, "Cases of Electronic evidence in Malaysian Court: The Civil and Syariah Perspective", *Proceeding of the International Conference on Social Science Research (ICSSR)* 2013 organized by WorldConferences.net, (e-ISBN 978-967- 11768-1-8), (Penang: WorldConferences.net, June 2013), 801.

[14] Fenner, G. Michael, "The Admissibility of Web-Based Evidence", *Creighton Law Review*, vol. 47, (2013): 70.

[15] Mason, Stephen, 25.

[16] Ibid.

[17] Ibid., 1.

[18] Electronic Commerce Act 2006 (Act 658), section 5.

The definition covers all types of statement or representation, including translation that is produced by a computer and displayed on the screen. Computer is defined as "any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by whatever name or description such device is called; and where two or more computers carry out any one or more of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer". When all term is combined, it can be understood that even when the term computer is being used, it includes all electronic devices when it refers to the electronic evidence[19].

It could be surmised that electronic document is any data that is associated with computer or electronic devices that can be created, stored, transmitted, and manipulated, either directly by computer generated or by human command. Data in e-mail need expert to validate who used the computer at that time or who is the sender of the e-mail, the owner of the e-mail account, the motive behind that, the authenticity or validity of the content, etc. especially with the data which is directly generated by devices. In other words, establishing the authenticity of electronic evidence is quite dependent with the computer forensic experts more than the data conducted with the human intervention. This also will differentiate between the levels of expert for both type of electronic document.

An illustration to the section 3 of the EA further illustrates the meaning of document which includes any writing, words printed, lithographed or photographed, a map, plan, graph or sketch, an inscription on wood, metal, stone or any other substance, material or thing, a drawing, painting, picture or caricature, a photograph or a negative, a tape recording of a telephonic communication, including a recording of such communication transmitted over distance, a photographic or other visual recording, including a recording of a photographic or other visual transmission over a distance, a matter recorded, stored, processed, retrieved or produced by a computer. The above definitions, can be used to further understand the meaning of "electronic evidence" in Malaysia. Electronic evidence is document that was created in digital format with the advancement of technology apart from the physical form[20]. Thus, it is submitted that

---

[19] Evidence Act 1950 (Act 56) (Amendment No 2 Act 2012), section 3 and Computer Crime Act 1997 (Act 563), section 2 (1).
[20] Mason, Stephen, 1.

electronic evidence is a type of documentary evidence that can be used by the prosecutor to prove the accused person is guilty.

2.1. Electronic Document from Islamic Perspective

Document in Islam is called *al-kitabah* or *al-khat, muharrar, asnad, hujaj, auraq, sukk, hujah, mukhadar, sijjil* and *wathiqah*. All of these terms refer to document in Islam[21]. Before this, document in Islam is just the written statements on paper or parchment manuscript for future reference or dispute[22]. The definitions given were based on their situations and time. However, the most important thing about document is about something that can be understandable, useful and contain information. Hence, in today's age, with technology and dynamic telecommunication and gadget, the need to expand the scope of documentary into digital and electronic cannot be denied as long as the data is understandable, useful and contain information[23]. Therefore, Islam would accept electronic document which is "any data that are associated with electronic devices that is created, stored, manipulated, or transmitted in digital format. Data in electronic format is data that can be understood, useful and contain information. The difference between data in digital format and non-digital format is the medium being used to create, process and store the data which is associated with electronic devices including computer or smartphone devices.

There are lots of provisions in al-Qur'an[24] and sunnah[25] that described the acceptance of *al-kitabah* as a means of proof. From the literature, Islamic jurists do not have similar opinion on *al-kitabah* as a means of proof[26]. Their concern is whether the documentary evidence or *al-kitabah* is forged. It is clear that *al-*

---

[21]Wan Abdul Fattah Wan Ismail and Zulfakar Ramlee, "Keterangan Melalui Kitabah: Menurut Fiqh dan Undang-Undang Semasa", *Jurnal Undang-Undang & Masyarakat*, (2013): 2; al-Zuhaily, Muhammad, *Wasail al-Ithbāt fī al-Syarᶜah al-Islamiyyah fī al-muᶜamalat al-Madaniyyah wa al-Ahwāl al-Syakhsiyyah*, (Bayrūt: Maktabah al-Muayyad, 1994), 2:416.

[22] For example, in the Qurān, Allah order people to write when debt to someone else which is could be understand that the written debt could be a proof or reference in future. (Refer al-Qurān, al-Baqarah, 282).

[23] Mohamad Ismail bin Hj. Mohamad Yunus, "Kedudukan Bahan Bukti (Exhibit) Elektronik dan Digital Dalam Keterangan: Masalah dan Cabaran Masa Kini", Insaf: The Journal of the Malaysian Bar, vol. 35, no.1, (2006):10.

[24] Al-Baqarah: 282; al-Naml: 28.

[25] Hadith about will. Ibn Umar reported Allah's Messenger ﷺ as saying: "It is the duty of a Muslim who has something which is to be given as a bequest not to have it for two nights without having his will written down regarding it" *Sahih Muslim* (Translation), Book 13, Kitāb al-Wasiyya (The Book of Bequests) Number 3987. via IIUM <http://www.iium.edu.my/deed/hadith/muslim/013_smt.html>.

[26] Bek, Ahmad bin Ibrahim, *Turūq al-Ithbāt al-Syarᶜiyyah maᶜa Bayān Ikhtilaf al-Madhāhib al-Fiqhiyyah.* Edit Wasil ᶜAla al-Din Ahmad Ibrahim, (al-Qāherah: Matbaᶜah al-Qāhira, 1985), 55. Majority of them which are Hanafi, Maliki

kitabah are accepted as a means of proof if there is no issue about the document being forged or the jurists will not argue in accepting it if the *al-kitabah* is proven authentic. Majority of them which are Hanafi, Maliki and some Syafie's and Hanbali's followers do not accept documentary evidence as a form of proof[27]. For them, *al-kitabah* can be subjected to falsification and forgery. This opinion shows that jurists do not reject documentary evidence totally. Their worry is *al-kitabah* is prone to falsification and forgery, but if the document can be ascertained authentic, there is no reason to reject that documentary evidence. At the same time, expert can clarify whether the *al-kitabah* is authentic or not[28]. It is similar with electronic evidence, whereby computer forensic experts can ascertain whether the digital data is authentic. It can be concluded that Islam accepted and recognized electronic evidence as an evidence under documentary evidence[29] subjected to the facts presented must be verified and assured of its authenticity and reliability by a person or persons normally known as expert witnesses.

Evidence in Islam is known as *bayyinah*. *Al-Bayyinah* can be further categorized as *al-shahadah* (testimony), *al-iqrar* (confession) and *al-yamin* (oath) as a means of proving a fact or facts. Apart from the three well accepted methods, *al-qarinah* (circumstantial evidence) and *al-kitabah* are additional methods that is also accepted in Islam as a means proving fact or facts. As facts presented to the court through these two methods which are *al-qarinah* and *al-kitabah*, human involvement to further clarify, verify and strengthen the evidence is compulsory. This is to ensure accountability and responsibility towards the facts presented to the court because in Islam, it is the human that is being held accountable toward the acts, not the evidence itself.

---

and some Syafie's and Hanbali's follower do not accepted documentary evidence as a form of proof because al-kitabah prone to forged. (See al- Syīraziyy, Abū Ishāq Ibrāhīm ibn ᶜAli, *Al-Muhazzab fī al-Fiqh al-Imām al-Syāfiᶜe*, (Bayrūt: Dār al-Kutub al-ᶜIlmiyyah, 1995), 3:401; Ibn Farhūn, Muhammad, *Tabsirah al-Hukkām*, (Bayrūt: Dār al-Kutub al-ᶜIlmiyyah, 1995), 1:304; Ibn Qayyim, *Iᶜlām...*, 204; Ibn Qudāmah, *al-Mughni*, 13:605. The other opinion which are from Maliki, some Ahmad's and some recent jurist accepted the admissibility of *al-kitabah* (Refer to: Al-Zuhaily, Muhammad, *Fiqh al-Qadā' wa al-Da'wa wa al-Ithbāt Dirāsah Muqāranah baina al-Mazāhib al-Fiqhiyyah wa Qawānin al-Imārah,* (University of Sharjah, Fakulty of Syariah and Islamic Study, 2002), 269-270; Ibn Farhūn, 303, Ibn Qayyim, *Al-Turūq ...,* 173, Ibn Muflih, Muhammad, *Kitab al-Furu'*, (Bayrūt: Mu'asasah al-Risālah, 2003), 11:227 & Ibn Nujaim, Zainuddin ibn Ibrahīm ibn Muhammad, *Al-Bahr al-Rā'iq Syarh Kunz al-Daqā'iq,* (Bayrūt: Dār al-Ihyā' al-Turāth al-ᶜArabiyy, 2002), 7:5.

[27] al-Syīraziyy, 401; Ibn Farhūn, at 304; Ibn Qayyim, *Iᶜlām ...,* 204; Ibn Qudāmah, *al-Mughni*, 13:605.

[28] Al-Syīraziyy, 401; al-Hasfakiyy, Muhammad ibn ᶜAli, *Radd al-Mukhtār ᶜala al-Dār al-Mukhtār Hāsyīah ibn Ābidīn*, (Bayrūt: Dār al-Maᶜrifat, 2000), 8:152.

[29] Duryana Mohamed and Zulfakar Ramlee, "C Cases of Electronic evidence in Malaysian Court: The Civil and Syariah Perspective", *Proceeding of the International Conference on Social Science Research (ICSSR)* 2013 organized by WorldConferences.net, (e-ISBN 978-967- 11768-1-8), (Penang: WorldConferences.net, June 2013), MMXIII, 805.

2.2 Characteristics of Electronic Document

Electronic document has its own characteristics compared with conventional document. It also opens a lot of unanswered questions to the users because they only see the data on the screen which is only a part of the data. The unanswered questions will be answered by the appearance of expert in this particular area, namely computer forensic or digital forensic investigator. It is also mysterious to many users because an expert can see what users cannot see and find what others cannot find. At the same time, in order to find or discover electronic evidence, there must be a tool such as software and hardware which is compatible with the computer or devices[30] or operating system being used. There are many characteristics of electronic document that will be mentioned below:

2.2.1 Easily Manipulated or Altered

Electronic document can easily be manipulated[31], altered, damaged or destroyed[32]. It can be modified without leaving a trace of the original message and need expert to clarify it, compared to record written with pen and paper[33]. Sometime, data or information can be accidentally or unwittingly modified by the user even without intention. Data in computer or electronic devices also could be damaged by the failure of the operating system, software and hardware. Even with the virus in the system and mishandling the computer to name a few, could alter or destroy the data. Even, the original electronic data could be destroyed or have a serious change while in the process of collecting. Hence, its authenticity is an issue. Therefore, it is very important to ensure that the electronic document is well preserved and protected. Some of the data has no evidentiary value and inaccurate because they are easy to create, copied, or

---

[30] Mason, Stephen, *Electronic Evidence,* 30*;* Guofu Ma and others, "Computer Forensics Model Based on Evidence Ring and Evidence Chain", *Procedia Engineering*, vol. 15, (2011): 3665. ScienceDirect via Procedia Engineering, <http://dx.doi.org/10.1016/j.proeng.2011.08.686>.

[31] Kuntze, Nicolai and Rudolph, Carsten, "Secure Digital Chains of Evidence," (paper presented at Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, California, USA, May 26, 2011).

[32] Pollitt, Mark M, "The Digital Crime Scene", in *Handbook of Digital and Multimedia Forensic Evidence*, ed. by J.J. Barbara (Totowa, NJ: Humana Press Inc, 2008), 65.

[33] Garfinkel, Simson L. "Providing Cryptographic Security and Evidentiary Chain-of –Custody with the Advanced Forensic Format, Library, and Tools", *International Journal of Digital Crime and Forensic,* vol. 1, no.1, (January –March 2009): 1.

manipulated[34]. It is clear that electronic document is easily altered either intentionally or unintentionally or even unwittingly.

The nature of electronic document itself, which is fragile create challenge to the cybercrime investigators to ensure successful prosecution. The evidence would be inadmissible or its weightage affected when any of the fragility happen. The data may "mutate" unintentionally when the computer is used during normal process by overwritten or overlaid by new user activity. It could be understood as Brenner and Frederikson mentioned "the simple act of starting a Microsoft Windows system will destroy more than 4,000,000 characters of evidence, and the spoliation will be far greater if the system is used to run any programs"[35]. It shows just how volatile is electronic document and its evidential value in court. Therefore, authenticity of electronic document must be proven otherwise it is not admissible in evidence.

2.2.2 Difficult to Eliminate

Electronic document is difficult to eliminate but easy to create. When a file or data on the computer is deleted, it does not mean that it is really gone for good, but it will be stored away or merely moved to another location in hard drive or digital storage devices or archive system[36]. It is because the computer contains metadata to enable the computer to retrieve the data which is supposedly deleted[37]. Sometime, the data is also overwritten after a period of time it is supposedly deleted. The data can be recovered with the intervention of the expert and can be used in the court of law[38]. It seems that the data are time-sensitive but the investigator or expert are able to recover the data which can be used in the court of law[39]. However, the question then is whether the recovered data are genuine or authentic or any other word 100% true without any spoliation or damages or mutation?

---

[34] Blazek, Zdenek, "Models of Investigation and Processing of Digital Evidence", *Digital Evidence and Electronic Signature Law Review*, vol. 5, (2008): 192; Wright, Jason T. and Wrabel, Scott, "Computer Forensic : Not Just for "Techies" Anymore", *Young Lawyer*, vol. 14, no. 9, (2010): 4.; Mason, Stephen, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), 195.
[35] Brenner, Susan W and Frederiksen, Barbara A, "Computer Searches and Seizures: Some Unresolved Issues", *Michigan Telecommunications and Technology Law Review*, vol. 8, (2002): 66.
[36] Rockwood, Rebecca, "Shifting Burdens and Concealing Electronic Evidence: Discovery in the Digital Era", *Richmond Journal of Law & Technology*, XII, (2005): 3.
[37] Ibid., 4.
[38] *Armstrong v. Bush*, 721 F. Supp. 343, 345 n.1 (D.D.C. 1989); *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280, 1283 (D.C. Cir. 1993).
[39] Yeager, Eric, "Looking For Trouble : An Exploration of How to Regulate Digital Searches", *Vanderbilt Law Review*, vol. 66, (2013): 718.

2.2.3 Metadata

Metadata is special characteristic in relation to electronic devices including electronic evidence. Metadata means data which is invisible or hidden behind a screen or display monitor[40]. Metadata is like a fingerprint and different for every data created[41]. It could be created by a user or automatically created by a program and store on the computer and make the user unaware of its existence[42]. For example, a photo that is captured by devices or camera automatically creating a data regarding the camera such as its model, setting of that camera and time the photo was taken[43]. The question is what if the camera setting data like year, date and time was wrongly done? It can make the court to erroneously exclude it. It is similar with the metadata in Microsoft Word document[44] with the setting of the person who register the product. Even when the computer is used by another person, it recorded with the person who is registered with it not the user. It brings a picture on how inaccurate the metadata itself can be. The primary issue is, who really is behind the screen and how to figure it out? For example, in *R v Cockell*[45], the expert (Constable Hancey) testified on the data relating to the digital photograph. He said that the date marked on a picture by the device could be off for any reason but the picture also contained metadata which was embedded information with picture in the device. Once embedded the information such as the date of creation, model used, etc. contained in the metadata did not change because metadata was the most reliable available information of the date of creation of a digital photograph even though there is no 100% certainty that data is correct.

Usually, metadata relates to the discovery of evidence and investigation process in obtaining evidence because the user cannot understand untold story. Computer forensic expert is a suitable person to detect

---

[40] Harris, Gretchen J., "Metadata: High-Tech Invisible Ink Legal Considerations", *Mississippi Law Journal*, vol. 78, no. 4, (2009): 950.
[41] Minnesota E-Discovery Working Group 3, "IT Technologies and How to Preserve ESI Cost Effectively", *William Mitchell Law Review*, vol. 40, (2014): 493.
[42] Wong, Denise H., "Educating for the Future: Teaching Evidence in the Technological Age", *Digital Evidence and Electronic Signature Law Review*, vol. 10, (2013): 18.
[43] Harris, Gretchen J., 944.
[44] Metadata in Microsoft Word document is information about author's name, date of file creation, number of word, tracks changes and everything about the file. The simplest way to view metadata in document is to go to File and then Properties but it does not show all the data that we need to know. Another way to see behind the screen with the another software such as Metadata Assistance, Workshare Protect or iScrub which is not only to remove metadata but also to discover metadata from others.
[45] [2013] A.J. No. 466.

and recover evidence behind the scene or invisible evidence[46]. This invisible data tells the story about who created, edited, printed, moved or whatever related with that file. However, authenticity is also an issue to metadata beside the accuracy of the information (truth of the contents) relayed by the metadata[47]. The point is, it is difficult to identify the actual user who is responsible with the actual action or who created or altered the data, which brings the issue of credibility of the electronic evidence itself[48]. In order to bring proper and authentic metadata in court, all aspects could be considered because metadata is related to a huge amount of data and it poses a big challenge to computer forensic to produce the accurate data in time either recovery, preserve and interpretation of the data. Probability to admit the data which has no evidentiary value or inaccurate is high based on the characteristic of electronic evidence and the challenge of the big data itself[49].

2.2.4 Recognition of User

Electronic data identify the online user by internet protocol (IP) address and not as a human. The architecture of the electronic devices itself make the user who will be known as IP address. IP address[50] is a numerical label assigned to each device which is address of a connected device in an IP network (Transmission Control Protocol[51] (TCP)/IP network). Every electronic device such as desktop and laptop computer, server, scanner, printer, modem, router, smartphone and tablet are assigned an IP address, and every IP packet traversing an IP network contains a source IP address and a destination IP address. Even though, an IP address are unique number[52] but it can be duplicated easily[53]. There are also possibilities where users can share an IP address. The architecture of electronic devices by IP address provides opportunity for criminals with hiding places behind the IP address as an anonymity user. Instead, there is more than one person behind that IP address. Therefore, it is quite a daunting task for the forensic

---

[46] Luehr, Paul H., "Real Evidence, Virtual Crime: The Role of Computer Forensic Experts", *Criminal Justice*, vol. 20, (2005): 15.
[47] Harris, Gretchen J., 963.
[48] Fenner, 63–98.
[49] Blazek, 194-195.
[50] Encyclopedia PC, "IP address", PC http://www.pcmag.com/encyclopedia/term/52610/, (accessed 14 February, 2013).
[51] The reliable transport protocol within the TCP/IP protocol suite.
[52] Keene, Shima D., "Financial crime in the virtual world", *Journal of Money Laundering Control*, vol. 15, no. 1, (2012): 33.
[53] Chen, Yinjie & ors "Identifying Cyber Criminals Hiding Behind Wireless Routers", (paper presented at Conference IEEE International Conference on Computer Communications Workshop (Infocom) organized by IEEE Infocom, Shanghai, China October 2011).

investigator to nail down the exact criminal because IP address is not unique like fingerprint, and IP address alone may not be insufficient to pinpoint the offender.

In *Patrick Collins, Inc. v John Doe*[54] Judge Spatt held that due to the prevalence of wireless routers, the actual device that performed the allegedly infringing activity could have been owned by a relative or guest of the account owner, or even an interloper without the knowledge of the owner. Therefore, IP address alone is insufficient to establish a reasonable likelihood [that] it will lead to the identity of defendants who could be sued, and the claim was dismiss, so do the complaint was denied. This case is about legal claim of copyright infringement, where plaintiff (Collin) claims that he is the owner of a copyright for the pornographic film "Gangbanged". He claims that defendant downloaded some or all of the Plaintiff's work using the BitTorrent Peer-to-Peer[55] sharing protocol. The plaintiff commenced the present lawsuit on March 8, 2012, alleging direct and indirect copyright infringement against nine anonymous Joe Doe which are identified only by their IP address.

From the above case, it is clear that if the only evidence is IP address, the court cannot make further action because IP address alone are not enough as identification evidence. Thus, IP address itself does not show identity of the person itself. Furthermore, an IP address can be easily stolen even by amateur hackers[56]. Hence, to avoid injustice to the person, in relation to the IP address alone as an evidence, the right decision is to dismiss or there is no further action about that claim. Research by Cisco reports that global IP traffic is expected to grow exponentially by overall will be nearly threefold or three times as many devices connecting to IP networks from 2013 and reach a total of 8.6 zettabytes[57] annually by 2018[58]. That is why IP address alone cannot convince the judge as far as the identity of the perpetrator is concerned.

It can be concluded that electronic document is very technical and complex for the user to understand as it has a unique nature compare to paper format. It is also volatile and easy to manipulate either accidentally, unwittingly or with intention and have an enormous volume with lower cost and time. All

---

[54] 945 F. Supp. 2d 367; 2013 U.S. Dist. LEXIS 71122.

[55] BitTorrent is a peer-to-peer protocol that allows users to transfer large files on the Internet.

[56] Chen, Yinjie et. al. "Identifying..., 1-14.

[57] A zettabyte is one billion terabytes. In Merriam Webster Online Dictionary means one sextillion bytes. (sextillion in value in power of ten is 10^{36}).

[58] Cisco Global Cloud Index: Forecast and Methodology, 2013–2018 White Paper, via Cisco, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html>.

these unique nature makes the necessity of chain of evidence relevant in order to ensure the electronic evidence is authentic and can be admissible in the court[59]. Proving the authenticity of evidence is a crucial aspect when it comes to electronic evidence. It contains the combination between technical aspect rather than litigation aspect. The technical aspect will lead to successful and strong evidence. It also will ensure that the evidence will be admitted.

3. ISSUES

There are many issues in relation to electronic document. Among them are authenticity, reliability, admissibility and dependency to the expert to name a few. These issues can be divided into three categories, namely authenticity, reliability and application of analyzing technique of computer forensic which is mentioned generally below: -

3.1 Authenticity Issue

Authenticity is the main issue in electronic document. It is because electronic evidence has a unique characteristic such as being easily manipulated and fragile. In order to ensure the authenticity or genuineness of the electronic document, an expert in technology or computer forensic is needed. They are suitable persons that can analyse and preserve the data. In order to ensure the authenticity of electronic document, the expert must be able to show the chain of evidence is not broken, this will prove the integrity of the evidence itself before it can be used to prove certain cases[60]. In *Alliance and Leicester Building Society v Ghahremani*[61], electronic evidence which is computer generated document is rejected as an evidence because its authenticity cannot be proven. Hirst LJ agreed with Hoffman J. in previous court concerning his judgement:

> "...but it is important to bear in mind that for Mr. Chopra's explanation to be true, a number of unlikely events must all have happened: for example, the truncated version

---

[59] Blazek, 192.
[60] Rowlingson, Robert, "A Ten Step Process for Forensic Readiness", *International Journal of Digital Evidence*, vol. 2, no. 3, (2004): 3.
[61] [1992] RVR 198 (Eng Ch Div). This case is about seeks an action about damages from the mortgagors for misrepresentation, and from the solicitors and values who acted in the transaction for professional negligence. Appellant (building Society) is attempting, for the third time, to obtain summary judgment against the solicitors for damages to be assessed. As a verdict, the case was dismissed with cost.

must have been created in the way he says, it must have escaped being overwritten by or itself overwriting the full version between March 1989 and 14th April 1991, the date of formatting the Compaq disc must be wrong, Mr. Goldmeier must have been mistaken and so on. The cumulative probability of all these things having been true is in my judgment almost negligible... I therefore find it proved beyond reasonable doubt that Mr. Chopra did alter or destroy part of the document and committed a contempt. It must also follow that he compounded his misconduct by subsequently forging a document which purported to show that the computer record had not been altered on 8th July."

The characteristic of the electronic evidence and the architecture of electronic format open to the many question whether traditional best evidence rules are still relevant because of the absent of original document in electronic format. At the same time, the necessity and dependant to the professional or expert in electronic devices or computer forensic is a must to ensure the originality of the document itself. Nobody can simply justify the originality of the document in electronic format by looking at the document. Therefore, authenticity of the electronic evidence is one of the major issues that need to be resolved.

3.2 Reliability Issue

Beside, reliability is also issues that need to look into completely. Reliability means the extent to which test or procedure yield the same results on repeated trials[62]. The output data need to be verified as a content of the document. The reliability can be indicated when the court get a consistent testimony by unrelated witnesses about a particular event included documentary and physical evidence[63].

3.3 Electronic Document Issues Summation

As mention earlier, the main issues concerning electronic document are authenticity and reliability, where the assurance of evidence presented are not portraying the true facts as well as fabricated. Electronic evidence is admissible in Malaysia with the amendment of EA in 1993. It is provided in section 90A with

---

[62] Merriam Webster Online Dictionary, An Encyclopedia Britannica Company, "reliability", https://www.merriam-webster.com/dictionary/reliability, (accessed 19 Jun, 2018).

[63] Thomson, Lucy L., "Mobile Devices: New Challenges for Admissibility of Electronic Evidence", *The SciTech Lawyer,* vol. 9, no. 3, Winter/Spring, (2013): American Bar Association.

seven subsections[64]. Section 90A (1) mentioned that electronic evidence or CGD should be produced by the computer in the course of its ordinary used. At the same time, the electronic evidence must comply with the definition of computer under section 3 of EA. For example, in *Hanafi Mat Hassan v PP*[65], an automated bus ticketing machine, a termalcycler and a DNA analyser were held to be computer generated document (CGD) and included within the meaning of definition of computer under section 3 of Evidence Act. The court dismissed the appeal by the accused (charge with rape and murder) and confirmed the conviction and sentence of High Court.

Electronic document or computer-generated document (CGD) can be divided into two, namely produced by a computer in the course of its ordinary use[66] and not produced by the computer in the course of its ordinary use[67]. "In the course of the ordinary use", the CGD can be proven by two ways as clarified by Shaik Daud Ismail JCA in *Gnanasegaran Pararajasingam v PP*[68].

1) it 'may' be proved by the production of the certificate as required by sub-s (2). Thus, sub-s (2) is permissive and not mandatory. This can also be seen in sub-s (4) which begins with the words 'Where a certificate is given under subsection (2)'; or
2) by calling the responsible person or maker of the document.

Sub-section (2) clearly states that a certificate is one of the methods to prove CGD in the course of ordinary use. The certificate shall be sufficient under section 90A (3) for a matter to be stated to the best of the knowledge and belief of the person stating it. It also shall be admissible in evidence as *prima facie* proof of all matters stated in it without proof of signature of the person who gave the certificate.

Tendering a certificate is one way to prove the electronic evidence, but it is not mandatory in all cases as explained in *Gnanasegaran* case[69]. In *Petroliam Nasional Bhd & Ors v Khoo Nee Kiong*[70] Su Geok Yiam JC stated that it is not compulsory for the plaintiffs to exhibit a certificate pursuant to section 90A in his affidavit in support of the plaintiffs' application in respect of the computer printouts containing the

---

[64] Evidence Act 1950 (Act 56), section 90A come into force on 15 July 1993.
[65] *Hanafi Mat Hassan v PP* [2006] 4 MLJ 134.
[66] Evidence Act 1950 (Act 56), section 90A (1).
[67] Evidence Act 1950 (Act 56), section 90A (6)
[68] [1997] 3 MLJ 1 at p.11.
[69] The terms 'may be proved' in section 90A (2) indicates that the tendering of a certificate is not a mandatory requirement in all cases.
[70] [2004] 2 LRC 202

impugned statements. The requirement to tender a certificate under section 90A is required only if the plaintiffs do not wish to call the officer who had personal knowledge of the production of the computer printouts by the computer to testify to that effect in the trial proper.

Instead, there are several ways of proving authentication in the MEA, which include calling the maker or the witness (Section 67) and expert opinion (Section 45), and comparing signatures (Section 73), and admission (Section 70) and by tendering the certificate (section 90A (2). However, the unique nature of electronic document poses a special way in investigation, preservation as well as the truths of its contents[71]. Electronic document can be authenticated by testimony of the witness. The witness can testify the data from the photo. For example in *Datuk Seri Anwar bin Ibrahim v Wan Muhammad Azri bin Wan Deris*[72] defendant denied that he is an author of all articles in any blog that has a URL in www.papagomo.com and he is not the owner of that blog. However, with the credible witness testimony (Mohd Fauzi bin Mohd Azmi (SP1)), which recognized the defendant as Papagomo when they meet at the Bloggers United Malaysia Conference on 16 May 2009 in Lake View Garden, Subang Jaya where he took the defendant's photograph. At that time, defendant admitted to the witness that he was the blogger named 'Papagomo'. Although, the defendant denied that he is the person in the photograph, the court believed that the person in the photo and the defendant was the same person. The court decided that the defendant had to pay RM800,000.00 to the plaintiff because the defamatory statements were extreme and were published widely. It is clear that without credible witness (Mohd Fauzi bin Mohd Azmi), it is difficult to prove the defendant is an author and owner of the blog. Even though there is a photograph of the defendant, without testimony from the witness, the defendant could could distant himself from the allegation. This situation happens because the anonymity of the virtual activity by internet user[73].The user can only be recognized by Internet Protocol (IP) address and not by the person itself. Even though, IP address is unique, but it can be duplicated easily[74]. Therefore, testimony of the witness (normally expert witness) can be the main method or form in authenticating electronic evidence.

---

[71] Borisevich, Galina and others, "A Comparative Review of Cybercrime Law and Digital Forensics in Russia, The United States and under the Convention on Cybercrime of the Council of Europe", *Northern Kentucky Law Review*, vol. 39, (2012): 292.

[72] [2014] MLJU 177, 9 MLJ 605 at 618. This case is about publishing the defamatory statement through the website www.papagomo.com.

[73] Keene, Shima D., "Financial crime in the virtual world", *Journal of Money Laundering Control*, vol. 15, no. 1, (2012): 33.

[74] Chen, Yinjie & ors "Identifying Cyber Criminals Hiding Behind Wireless Routers", (paper presented at Conference IEEE International Conference on Computer Communications Workshop (Infocom) organized by IEEE Infocom, Shanghai, China October 2011).

It is difficult to identify the real author or creator of the electronic publication or evidence in electronic format[75] In order to ensure the authenticity of the electronic evidence, it is implying an attribute of identity of the user or owner of the data[76]. The constancy of the data in a record (integrity of the data) and time information related to the object is correct is also important. In order to prove the authentication of electronic evidence, there are two aspects that must be looked into, namely, chain of evidence and second, the data have not been modified or replaced between the time it was created or added to the moment they were required[77]. Since digital evidence is complex, diffuse, volatile and can be accidentally or improperly modified after acquired, the chain of custody must ensure that collected evidence can be accepted as truthful by the court[78]. Therefore, the authenticity must be proven[79]. Chain of custody of such evidence is also one of the methods to ensure the electronic document is authentic and accepted by the court from the time the data created till the time it required[80].

In *Mohd Ali Jaafar v Public Prosecutor*[81], the appellant was found guilty by the session court judge. In this case, learned counsel for the appellant contended that the chain of custody of the tape recordings has not been established by the prosecution. He said that this must be affirmatively proved and, in support, referred to *Ghazali bin Salleh & Anor v PP*[82] . Augustine Paul J, said that the authenticity of the recordings had not been proved. Therefore, the tape recordings were wrongly admitted in evidence by the judge. As the conviction of the appellant on the first charge was anchored on the recorded evidence, it could not be sustained. Accordingly, the conviction and sentence on the first charge was quashed.

---

[75] *Datuk Seri Anwar bin Ibrahim v Wan Muhammad Azri bin Wan Deris*, [2014] MLJU 177, 9 MLJ 605 at 618.

[76] Paul, George L., *Foundations of Digital Evidence*, (United State of America: American Bar Association, 2008), 35-36.

[77] Mason, Stephen, *Electronic Evidence*, 89.

[78] Giova, Giuliano. "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems", *International Journal of Computer Science and Network Security*, vol. 11, (2011):1.

[79] Adv R Lekala, "E-mail Communication for Provisional Sentence Summons", *Journal of International Commercial Law and Technology*, vol. 6, no. 3, (2011): 149.

[80] Xindong Wu and others, "Data Mining with Big Data", *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no.1, (2014): 99. IEEE Xplore via Digital Library <https://doi.org/10.1109/TKDE.2013.109>; Mason, Stephen, *Electronic Evidence*, 89.

[81] [1998] 4 MLJ 210 at 229. In this case, accused was charged for soliciting sexual favour from the complainant under s 3(a)(ii) of the Prevention of Corruption Act 1961 and for attempting to obtain sexual favours under s 4(a) of the similar Act.

[82] [1993] 3 CLJ 638.

There are many forms to authenticating electronic evidence such testimony of witness, admission, expert opinion and chain of evidence. There is no prima facie case if the case is solely dependent on electronic evidence[83] unless the accused pleaded guilty[84]. In order to ensure the authenticity of electronic document, the expert must be able to show the chain of evidence which will prove the integrity of the evidence itself before it can be used to support a legal process[85]. The expert must be careful and avoid any alteration during the process of searching, collecting, analyzing and presenting the data to the court.

The role of expert opinion is to assist the court in forming opinion because the court cannot form an opinion on the non-tangible evidence. This is due to the nature of electronic evidence which is in embedded or in hidden form. Generally, opinion evidence is not relevant because witnesses are only supposed to adduce facts not to give opinion. Giving opinion is the function of the court.

To date, Malaysia does not have safeguarding provisions in relation to authentication and credibility of electronic document compared with Singapore, Canada and United States of America. For example, in Canada Evidence Act stated: "Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.[86]" In Malaysia, it is just by way of calling the maker or tendering a certificate to that effect. Both Singapore and India have a very accommodative but cautious provisions in relation to authenticity of electronic evidence. Section 116A (2) of Singapore Evidence Act states that: "Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the electronic record" That sub-section mentioned that if a defendant seeks to adduce electronic evidence against plaintiff, the court will presume that the evidence

---

[83] *PP v Mohd Abdul Azizi bin Ibrahim* [2013] MLJU 530. This is murder case.
[84] *PP v Muhammad Nuzaihan bin Kamal Luddin* [2000] 1 SLR 34. Accused pleaded guilty under unauthorised access to computer materials, unauthorised modification of the contents of a computer and unauthorised access to a computer service under s 3(1), 5(1) and 6(1)(a) of the Computer Misuse Act (Cap 50A, 1993 Ed) ('CMA'); In *PP v Law Aik Meng* [2007] 2 814, [2007] SGHC 33, an accused pleaded guilty under Computer Misuse Act and Penal Code for working in syndicate involved in perpetrating ATM card fraud.
[85] Rowlingson, Robert, "A Ten Step Process for Forensic Readiness", *International Journal of Digital Evidence*, vol. 2, no. 3, (2004): 3.
[86] Evidence Act (Canada), section 31.1.

is authentic as a relevant fact as long as the electronic evidence was generated, recorded or stored in the usual and ordinary course of business by someone else which is neutral third party. It is also as a relevant fact for the court to presume that electronic evidence is authentic. The Singapore court will presume that the electronic evidence is authentic as long as the electronic evidence was generated, recorded or stored in the usual and ordinary course of business by someone else which is neutral third party. It is also a relevant fact for the court to presume that the electronic record is authentic. The court also presume the electronic evidence is authentic if the electronic evidence was generated, recorded or stored by a party who is adverse in interest to the party seeking to adduce the evidence[87] stored by the person who want to adduce evidence against the interest to the party.

In India, section 59 said that all the fact can be proved by oral evidence except the content of electronic evidence[88]. However, all the content of electronic evidence also can be proved by oral evidence and relevant if the authenticity of that evidence can be produced[89]. It is stated in section 22A[90]:"Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question." In order to prove the content of electronic evidence, India's section 65A mention clearly the way to do it which is in accordance with procedure prescribed under section 65B. Section 65B is about admissibility of electronic evidence. All the computer output which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document if it is satisfied with the four technological condition in sub-section 65B(2)[91]. Sub-section 4 of section 65B also gives a clear explanation in order to establish the authenticity of electronic evidence. The provision requires the certificate of a responsible person for the computer or devices on which the electronic record was created or stored as an additional condition for sub-section (2) of section 65B. The certificate must identify the original electronic record, describe the kind or manner of its creation and the devices that created it and certify with the compliance with the condition of sub-section 65B. The certificate also must be signed by a responsible person in relation to the operation of the relevant devices with their best knowledge and belief. It means that the certificate is unique in order to identify the evidence produce before the court in digital format.

---

[87] Evidence Act 1872 (Singapore), section 116A (2).
[88] Evidence Act 1872 (India), section 59.
[89] *Anvar v Basheer*, Civil Appeal no 4226 of 2012.
[90] Evidence Act 1872 (India), section 22A.
[91] Evidence Act 1872 (India), section 65B (1).

Canada, Singapore and India cautiously accommodate electronic document in evidence because electronic evidence is prone or susceptible to alteration, tampered etc. At the same time, the expert can be an examiner when authentication issue has been questioned[92].In *R v Petersen*[93], the court said that in order that electronic document is admissible in evidence, the party must offer some evidence of the authenticity of the document. Electronic evidence is inadmissible without any supported evidence to show its authenticity or genuineness[94]. In addition to proving the authenticity of the document, the proponent of electronic evidence must also demonstrate its reliability. The reliability of the electronic evidence can be demonstrated through tendering the certificate signed by a person responsible for the operation of the computer or electronic devices.

It shows that laws have to provide for warranted indulgences to accommodate the admissibility of electronic document i.e. it is authentic by calling the maker or through certificate, deeming provision such as stating it to be primary evidence, deeming it to be correct by presumption. These indulgences would circumvent or be in accordance with requirement of authentication, the best evidence rule, the rule against hearsay, as far as documentary evidence is concerned. Without these provisions, electronic document would have problems for it to be adduced in court.

4. CONCLUSION

Electronic document is a form of documentary evidence in addition to other type of evidence like direct evidence, circumstantial evidence and real evidence. Electronic document is fragile but indulgences have been given by law to boost its credibility, authenticity, primacy, weightage i.e. presumption as to its accuracy or correctness. Electronic document being a document have also been given indulgences that it is primary document to circumvent the best evidence rule (see section 64). It is important because when proof is by document, primary evidence applies unless exception applies (see section 65 of MEA). In this respect, MEA provided that electronic evidence is primary evidence (section 62). With regard to its weight or credibility (section 90A) the contents are deemed to be correct. These are examples of indulgences or accommodating provisions for the reception of electronic evidence in electronic format. In order for electronic document to be admissible in evidence, and to have the necessary weightage, it must first be

---

[92] Evidence Act 1872 (India), section 45A. (opinion of examiner of electronic evidence).
[93] [1983], 45 N.B.R. (2d) 271 at 282-85, 249-96. In this case an electronic evidence is videotape.
[94] *R v Rahkola*, [1979] 5 W.W.R. 464 at 466 (B.C.C.A.).

authentic which can be done by calling the maker or tendering a certificate. Therefore, the acceptance of electronic evidence in Malaysian courts is no longer an issue. Both Islamic law and common law are equally concerned when the evidence to be adduced is a document by requiring its authenticity be proven as a condition of its admissibility whether it is traditional or electronic document. While the law of evidence must accommodate electronic document, it is also equally important to update the existing authentication provisions of electronic evidence in Malaysian Evidence Act (MEA) 1950 to ensure that the authenticity of electronic document must be supported by evidence capable of supporting a finding that the electronic document is that which it is purported to be. In other words, it must be cautiously admitted in evidence.