Pertanika J. Soc. Sci. & Hum. 23 (S): 153 – 168 (2015)

PERTANIKA JOURNALS

SOCIAL SCIENCES & HUMANITIES

Journal homepage: http://www.pertanika.upm.edu.my/

Authentication of Electronic Evidence in Cybercrime Cases Based on Malaysian Laws

Mursilalaili Mustapa Sa'di[1], Abdul Rani Kamarudin[2], Duryana Mohamed[2]* and Zulfakar Ramlee[2]

[1]Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Department of Legal Practice, Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia

ABSTRACT

Electronic evidence is one of the many forms of documentary evidence. It is stored and retrievable from electronic devices such as computers and smartphones, particularly in the their hard disks or memory banks. However, due to the fragile nature of electronic evidences, it is prone or susceptible to damage or alteration, as well as destruction due to improper handling or safe keeping. Since it can easily be tampered with or self-deteriorate, establishing the authenticity and reliability of electronic evidence is a technical task. Meanwhile, states of affairs would cause such electronic evidence to be inadmissible or carries low or no weightage whatsoever by the court, thus undermining the prosecution's or the plaintiff's case, as the case may be. In order to ensure such evidence is admissible and carry the expected weightage, relevant parties must first prove the authenticity of such evidence and subsequently on its reliability and relevancy. Nevertheless, in cybercrime cases, proving the crime is actually a technical challenge, where the responsible personnel are required to understand what is electronic evidence, how to extract and preserve the originality of such evidence and the laws governing electronic evidence, as well as cybercrimes. This article attempts to explain the scope of electronic evidence in relation to criminal cases such as in cybercrimes, as far as its admissibility and weightage are concerned. The discussion will be based on Malaysian and common laws.

ARTICLE INFO

Article history:
Received: 21 April 2015
Accepted: 10 September 2015

E-mail addresses:
mduryana@iium.edu.my (Duryana Mohamed),
rani@iium.edu.my (Abdul Rani Kamarudin).
mursilalaili@yahoo.com (Mursilalaili Mustapa Sa'di)
* Corresponding author

ISSN: 0128-7702

Keywords: Authenticity, cybercrime and electronic evidence

INTRODUCTION

Electronic evidence is not a recent thing. It has been around for quite sometime in

the form of black box in aircraft, closed-circuit television (CCTV) in buildings and premises, at traffic junctions, desktop computers, laptops and smartphones. The contents stored in the hard disk and memory card (internal storage), whether they are in smartphones, televisions or computers, are generally known as electronic evidence. The same may be extractable and readable through their appropriate devices or in intricate situations, expert opinion is allowed to be given. Nowadays, with their portability and efficiency, and further advancement that electronic gadgets bring, whereby anyone is able to communicate with ease and speed, our dependency in the day-to-day affairs to electronic gadgets cannot be denied. It could improve and enhance the quality of life. However, with the advantages that the gadgets bring where anyone is able to communicate across geographical boundaries in real time, conduct business and transaction without physical presence, it also brings along with it disadvantages. It has also given criminals the opportunity to perpetrate their crimes through the internet (O'Donnell & Milner, 2009). These crimes are known as cybercrimes. All cybercriminal activities can be traced and trailed if one knows the technical nature of electronic evidence and how gadgets such as computers and smartphones operate. However, the downside of electronic evidence is that it can be easily altered and manipulated (Kuntze & Rudolph, 2011).

THE BRIEF LAW ON ADMISSIBILITY OF DOCUMENTARY EVIDENCE

Sections 45 to 51 of the Malaysian Evidence Act 1950 (MEA) are provisions whereby expert opinion as to the contents of those electronic evidence are legally relevant in cases where the court could not form an opinion in matters of art, science or foreign laws. Electronic evidence is also documentary evidence whereby prove must be by primary evidence as required by Sections 61 and 64 of MEA, unless exceptions apply under Section 65 of MEA. Under Section 65 of MEA, secondary evidence may be adduced, provided the person adducing it lays down the legal foundation as to why primary evidence is not available after having made a diligent search to procure the same. Electronic evidence, being also documentary evidence, must also be proven in terms of its authenticity in a manner provided under Sections 67 to 73 of MEA. Furthermore, for a document generated by computer, under Section 90A MEA (subject to its relevancy, best evidence rule and authentication), certification by the person in charge or managing the computer in its ordinary use and that the computer is in good working order, renders the document admissible. Section 90A considers computer generated documents (CGD) as primary evidence and also as an exception to the rule against hearsay.

CYBERCRIMES

To date, there is no standard definition of cybercrime. The terms "cybercrime,"

"computer crime", "Information Technology crime,", "high-tech crime", "internet crime" and "information Age Crime" are often used interchangeably (Clancy, 2011) to refer to the two major offences either computer as a target and traditional offences by means of computer or computer as a tool (Goodman, 1997). There are also computers that function as a container or storage of a valuable data on the crimes (Clancy, 2011). For example, when a blackmailer uses a computer to generate blackmail letters or email exchanges (Brenner & Goodman, 2002), the computer will keep and store the data. Cybercrimes could be understood as crimes that involve computer, computer system and other electronic devices either as a medium in which computers and electronic devices that are connected to the Internet or computer networks are used as the instrument to commit crime or as a target in which the computer or electronic devices are used to access data stored in the electronic devices (Kam Wai, 2006). Cybercrime activities also include those of 'traditional crimes', where criminals have found new ways in executing their criminal activities through the Internet by means of computer and other electronic devices (Stefan, 2011) and true cybercrimes which done using the technology (Brenner, 2007). Therefore, cybercrimes could be defined as "any activities that can bring harm by network technology for the purpose of manipulation of information or gain either by using computers or electronic devices as a tool, target or container" (Clancy, 2011).

Cybercrime differs from traditional crime by means of how the crimes are orchestrated. The main criterion that differentiates cybercrime and traditional crime is that the cybercrime is committed through an electronic device (Kam Wai, 2006), be it a desktop computer or a notebook, a cellular phone, tablet, etc. Another criterion is that criminal activities are committed remotely (Internet) compared to traditional crimes that require criminal's physical presence. Since cybercrime could be committed remotely, and there are no geographical and political boundaries in the cyber world, a cybercrime could also be transnational, since it affects not only one nation but several nations, making identification of crime scene location a difficult task. Meanwhile, Garfinkel (2009) states that cybercrime is a crime where the crime scene is `invisible'. It can be a heaven to cybercriminals because the percentage being caught of their cybercrimes is relatively small. Gabrys (2002) mentioned that there is less than a 1:20,000 chance of cybercriminals being caught and there is less than a 1:22,000 chance that the cybercriminals will go to prison. The reason being cybercriminals committed cybercrimes remotely without their physical present. However, there are electronic trails known as electronic evidence. Getting this electronic evidence is a technical challenge which investigators, defence counsel judges and lawyer must be familiar with, or they would face the problem in making decisions on it (Rockwood, 2005).

NATURE OF ELECTRONIC EVIDENCE

Electronic evidence is any data associated with electronic devices, whether created, stored, manipulated or transmitted in digital format. Electronic evidence is also known as digital evidence, computer evidence, computer generated document or computer-related document. The prime element of an electronic evidence which is an evidence is creating, storing, manipulating or transmitting in digital format with the advancement of technology tool (Mason, 2011).

There is no specific definition on electronic evidence under the Malaysian law, but it could be figured out in three different statutes, namely, the Electronic Commerce (ECA) 2006, Computer Crimes Act 1997 (CCA) and Malaysian Evidence Act 1950 (MEA). ECA in Section 5 defines electronic as any technology that can be used by various functions which is related to the technology. It could be computer and other devices such as a smart phone, tablet, iPad, etc., while 'computer output' is described in Section 2(1) of the CCA, which covers all types of statements or representations including translations that are produced by a computer and displayed on its screen. Section 3 of MEA provides the meaning of evidence and document. An illustration in that Section gives further understanding what a document is, which includes any writing or 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. Hence, electronic evidence is a form of documentary evidence.

Characteristics of Electronic Evidence

Electronic evidence is unique in its character compared to traditional evidence. Electronic evidence is easily manipulated (Kuntze & Rudolph, 2011), altered, damaged or destroyed (Pollitt, 2007). It can be modified without leaving any trace of the original message and it needs an expert to clarify it compared to record written with pen and paper (Garfinkel, 2009). The data in electronic format are also difficult to eliminate but easy to create. When a file or data on the computer was deleted, it does not mean that it is really gone as it will be stored away or merely moved to another location in the hard drive or digital storage device or archive system (Rockwood, 2005). It is because the computer contains metadata to enable the computer to retrieve the data which are supposedly deleted (Rockwood, 2005). Metadata means data which is invisible or hidden behind a screen or display monitor (Harris, 2009). It could be created by a user or automatically created by a programme and stored on the

computer and the user is probably unaware of its existence (Wong, 2013). Volume and speed of electronic data can be increased exponentially compared in paper format (Chung & Byer, 1998; Ahmad, 2008). The great volume of electronic evidence or too much quantity makes timely investigation an insurmountable task (Maurushat, 2010). To date, it has been a challenge for investigators to extract useful information from a large volume of data because the era of Big Data has arrived (Wu, Zhu, Wu, & Ding, 2014). Big Data refers to a buzzword or catch-phrase that is used to describe a massive volume of both structured and unstructured data that are large and difficult to process using traditional data base and software techniques. An example of Big Data is petabytes (1,024 terrabytes) or exabytes (1,024 petabytes) of data consisting of billions to trillions of records of millions of people - all from different sources (e.g., web, sales, customer contract, centre, social media, mobile data and so on). The data are typically and loosely structured data that are often incomplete and inaccessible (Beal, n.d.). Hence, finding data in a Big Data could be like finding a needle in a haystack, which is tedious for the investigator. In order to solve this problem, the investigator may need to use effective tools to investigate the crime such as the Big Data analytics (Armending, 2013).

It can be concluded that electronic evidence is very technical and complex for the user to understand as it has a unique nature compared to the paper format. It is also volatile and easy to manipulate either accidentally, unwittingly or wittingly and has an enormous volume with higher cost and time (Adams, 2011). 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. However, in order to ensure the authenticity of electronic evidence, 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 (Rowlingson, 2004).

AUTHENTICATION OF ELECTRONIC EVIDENCE FROM THE MALAYSIAN PERSPECTIVE

"Authentic" in *Merriam Webster Dictionary* means original, real or genuine, true or just like the original (http://www.merriam-webster.com/dictionary/authentic). The authentic characteristic of electronic evidences is difficult to achieve because data in electronic format are prone to alteration, modification and could be corrupted through extraneous factor such as virus or malware. The data, which are in an electronic format, will need to be interpreted because they exist in the binary form. Authentication in digital format can be understood as 'matches the claims made about it' (Pattenden, 2009) and not a fabricated data (Radhakrishna, 2009) or spoliation (Adams, 2011). Adam (2011) defines spoliation as the destruction or significant alteration of evidence based on case *West v. Goodyear Tire & Rubber Co*.,

167 F.3d 776, 779 (2d Cir. 1999). To date, there has been no authentication term in Malaysia concerning electronic evidence but there are modes of authenticating it. Authentication is different from encryption. The word encrypt is defined as 'to change (information) from one form to another especially to hide its meaning' ((http://www.merriam-webster.com/dictionary/authentic). Both authentication and encyrption are considered as two intertwined technologies that help to ensure the data to remain secured (Brenton, n.d.).

In Malaysia, there are two legal issues concerning electronic evidence. Firstly, whether particular electronic devices come under the definition of computer in Section 3 of the MEA. Secondly, whether a certificate needs to be tendered when a maker of a document is not called to testify in court. In *Hanafi Mat Hassan v PP* [2006] 4 MLJ 134, an automated bus ticketing machine, a termalcycler and a deoxyribonucleic acid (DNA) analyser were found to be computer generated documents. Those documents were admitted in the court although no certificate was produced to prove the authenticity of the ticket and the DNA report. The court dismissed the appeal of the accused who was charged with rape and murder and confirmed the conviction and sentences of the High Court. In *Gnanasegaran a/l Pararajasingam v PP*, [1997] 3 MLJ 1 at p.14, the Court of Appeal gave a clear clarification on whether a certificate had to be tendered under Section 90(A) of MEA. Mahadeve Shankar JCA held that Section 90A was enacted to bring "the best evidence rule" up to date with the realities of the electronic age. The effect of Section 90A(1) means that the computer generated document (CGD) is admissible and it is no longer necessary to call the actual teller or bank clerk who keyed in the data to come to court, provided he issued a certificate stating to the best of his knowledge and belief that it was made in the course of its ordinary use. The court also held that as the maker was in court to testify, the certificate is not necessary to be adduced. Apart from being primary evidence, the best evidence rule is somehow relaxed when it comes to electronic evidence. It too is an exception to the rule against documentary hearsay. Section 90B requires the court to give the admissible evidence the requisite weightage.

Electronic evidence or computer generated document can be divided into two, namely, produced by a computer in the course of its ordinary use and not produced by the computer in the course of its ordinary use. Shaikh Daud Ismail JCA clarifies that there are two ways to proving 'in the course of the ordinary use' of the computer in *Gnanasegaran a/l Pararajasingam v PP* [1997] 3 MLJ 1 at p.11. In the course of the ordinary use, it may be proven by the production of the certificate as required by sub-section (2). Thus, sub-section (2) is permissive and not mandatory. This can also be seen in sub-section (4) which begins with the phrase, "Where a certificate is given under sub-section (2)", or by calling the responsible person or the maker of the document.

However, tendering a certificate was not mandatory in all cases, as explained in *Gnanasegaran* case which used the words 'may be proved' in Section 90A(2) indicating that the tendering of a certificate is not a mandatory requirement in all cases. In *Petroliam Nasional Bhd & Ors v Khoo Nee Kiong* [2004] 2 LRC 202, 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 impugned statements. The requirement to tender a Section 90A certificate will only arise if the plaintiffs did 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.

From the above cases, it could be surmised that authenticating of electronic evidence in Malaysia can be done in two ways; either by the production of the certificate as required in Section 90A(2) or by calling the maker or the responsible person. In *PP v Goh Hoe Cheong & Anor* [2006] MLJU 468, the accused were charged under Section 39B(1) (a), Dangerous Drugs Act 1952. The electronic evidence, which were the baggage tag and a baggage claim tag were inadmissible in evidence in the absence of both oral evidence from Malaysia Airlines (MAS) or the authority managing Kuala Lumpur International Airport (KLIA) to prove the aspect of physical checking and any certificate under Section 90(1). The failure to authenticate CGD by adducing the certificate that the computer is in good working order and was produced in the course of its ordinary use would make an electronic evidence inadmissible in evidence under Section 67 of MEA. As a result, the accused were acquitted and discharged because the prosecution had failed to prove the charge against them.

Similarly, in *PP v Mohd Abdul Azizi bin Ibrahim* [2014] 10 MLJ 824 at para 62, when the court held that the closed-circuit television (CCTV) recording was inadmissible in the absence of both the certificate as well as the oral evidence for non-compliance with Section 90A of the MEA 1950. In this case, the electronic evidence was the hard disk in the CCTV. Even though it was not damaged and was able to vividly broadcast recording of the crime and was in safe custody, without adducing a certificate or oral evidence, it is inadmissible. Without the evidence of the CCTV recording, the prosecution had failed to establish that it was the accused who had caused the death of the deceased. Consequently, the accused was acquitted and discharged without calling the accused to enter his defence.

It is clear that there are methods in authenticating electronic evidence in Malaysia. Under Section 90A, electronic evidence can be admitted through one of two ways; either by tendering a certificate as stated in Section 90A(2) and (3) or an oral testimony to prove the document was produced by the computer "in the course of its ordinary use". It is followed by the

presumption in Section 90A(4) that the computer is in good working order and operating properly at the material time. The question is who will ensure that the computer or particular devices were properly functioning at the material time? Even though the computer was in the cause of its ordinary use, it is not impossible that at the material time, it was not in good working order or failed to operate properly (Mason, 2011). Even though in *DPP v McKeown; DPP v Jones*, Lord Hoffmann, [1997] 1 All ER 737 at 742, said that "it is notorious that one needs no expertise in electronics to be able to know whether a computer is working properly", it is an extreme view because it is not impossible to know that a computer is working properly even for an expert. Moreover, with the ability of cybercriminals to hack the computer system would depend on the expert to ensure that the computer is working properly. It shows the dependency to the expert in clarifying the electronic devices are in good working order.

Unfortunately, there is no specific provision in MEA on the authentication of electronic data or evidence compared to the United States (US) Federal Rules of Evidence in Rule 901 and Singapore Evidence Act (Amendment) 2012 in Section 116A, which repealed Sections 35 and 36. Other laws such as the United Kingdom (UK) Civil Evidence Act 1968 (CEA), the UK current civil evidence legislation, i.e. the Civil Evidence Act 1995 (CEA) and the UK Police and Criminal Evidence Act 1984 (PACE) also recognise the admissibility of electronic data and the importance of authenticating the data. Although there are provisions in MEA on authenticating a document under Sections 67 to 73A, the absence of specific provisions on electronic evidence has given rise to misunderstandings as to its admissibility or weightage (Radhakrishna, Zan, & Khong, 2013). Although the certificate or oral testimony is one of the means of authenticating electronic evidence, particularly computer generated document, it is not sufficient to ensure the originality and genuineness of electronic evidence. In the Supreme Court of India, Kurian J., in *Anvar P.V. v P.K. Basheer and others* Civil Appeal No. 4226 of 2012, observed that "electronic records being more susceptible to tampering, alteration, transposition, excision, etc., without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice". In this case, electronic evidence by way of secondary evidence such as printouts, compact discs (CDs), pen drives, micro-chips, etc., shall not be given and used as evidence unless the requirement of Section 65B of the Indian Evidence Act (IEA) is satisfied, which requires the person in-charge of the duplication of data to give the court a certificate that the data are authentic to the best of his or her knowledge. It is to be noted that Section 65B of IEA is *pari materia* with Section 90A of MEA 1950.

The issues of collection, preservation and discovery are also important to ensure the authenticity of the contents of

the electronic evidence. The court must look into the importance of preserving electronic evidence to ensure that the contents of the electronic evidence are also authentic (Haneef, 2006). It seems that people who are associated with the justice system must equip themselves on the reality of electronic evidence, i.e. the unique characteristic which is prone to damage and alteration (Garrie & Gelb, 2010). This is because they can properly address the issues that come with it.

Modes of authenticating electronic evidence

In order to ensure electronic evidence is admissible, the parties involved must not only prove that the electronic evidence is both relevant and authentic. 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). However, the unique nature of electronic evidence poses a special way in investigation, preservation as well as authentication of its contents (Borisevich *et al*., 2012). Electronic evidence can be authenticated by the following modes:

1. Testimony of the witness

The witness can testify the data or evidence from the photo. For example in *Datuk Seri Anwar bin Ibrahim v Wan Muhammad Azri bin Wan Deris* [2014] MLJU 177, 9 MLJ 605 at 618, the defendant denied that he is the author of all the articles in any blog available at the following URL, www.papagomo.com, and that he is not the owner of that blog. The defendant was accused for publishing the defamatory statement of the plaintiff through the website www.papagomo.com. However, there was a credible witness testimony [Mohd Fauzi bin Mohd Azmi (SP1)], which recognised the defendant as *papagomo* when he and the defendant met at the Bloggers United Malaysia Conference on 16 May 2009 at Lake View Garden in Subang Jaya, where he took the defendant's photograph. At that time, the defendant admitted to the witness that he was indeed the blogger named 'Papagomo'. Although the defendant denied that he is the person in the photograph, the court has a base to believe that the person in the photograph and the defendant are the same person based on the observation of the court. As a result, the defendant was ordered to pay RM800,000.00 to the plaintiff because the defamatory statement could be attributed to the defendant.

It is clear that without any credible witness (i.e., Mohd Fauzi bin Mohd Azmi), it is difficult to prove the responsible person or defendant being the author and owner of the blog. Even with the photograph of the defendant, without the testimony from the witness, the defendant could have easily denied that he was the writer named papagomo who had published the defamatory statement of the plaintiff through the website www.papagomo.com due to the anonymity of the virtual activity by internet user (Keene, 2012).

The user only can be identified through the Internet Protocol (IP) address and not by the person. Thus, there is a great challenge for investigator to identify the user of the electronic device. Even though the IP address is unique, it can be easily duplicated (Chen *et. al.*, n.d). In other words, cybercriminals can hide behind the IP address as an anonymous user. Cybercriminals do not use their real identification when committing any offence. Therefore, the testimony of the witness can corroborate the electronic evidence.

It is clear that in order to establish an authentic electronic evidence (photograph), expert opinion or a specialist in that subject is required to verify whether or not the photograph has been modified (Low, 2012). There are various types of software used in editing electronic pictures. However, identifying the authenticity of such pictures is a challenging task. This shows that electronic data including electronic photograph can be easily altered by using other technology. Apart from the testimony of witnesses, the testimony from the victim can authenticate electronic evidence. In *Kevin Michael Shea v The State of Texas*167 S.W.3d 98; 2005 Tex. App. LEXIS 3091, the accused (Shea) was convicted for indecency with a child. The victim's testimony authenticates the emails sent to her by the accused. The victim is familiar with the defendant's e-mail address and the contents of the e-mails match the conversation between them. In specific, the victim testified that the defendant had called her to confirm that she had received his e-mail. As a result, the court accepted the electronic evidence (emails) with the corroboration with other evidence. This overruled the objection raised by the defendant who had argued that the emails lacked of authenticity. On the other hand, the High Court of Kuala Lumpur in *Re Ng Liang Shing: ex-parte Sirim Bhd.* [2013] 8 MLJ 916 dismissed an appeal made by the Judgment debtor (JD) who relied on computer evidence and emails. The learned judge said, "Although the judgment creditor (JC) had not objected to the authenticity and the admissibility of JD's electronic evidence, nevertheless, for such evidence to be admitted, it would also require the evidence to be tested against the normal rules of evidence on burden and standard of proof and the weight to be attached to the evidence. The court found the relevance and weight to be given to the e mail trail and the electronic attendance record to fall far short of proof that the JD was actually in his department when the bankruptcy notice was purportedly served on him".

2. Expert Opinion

Section 45 of the MEA defines an expert as a person who has a special skill or knowledge or experience in science or art or foreign law which is acquired through special study or practice in that particular area. This means expert witnesses are able to give opinion(s) based on their skills for the questions asked. In *Chou Kooi Pang & Anor v Public Prosecutor* [1998] 3 SLR 593, Yong Pung How CJ opined that the expert opinion was only admissible to furnish the court with scientific information which was likely to

be outside the experience and knowledge of a judge. An expert must be skilled in his field whether through special study or from experience in order to assist the court.

Electronic evidence is a combination of law and technology, and the authentication of its contents has to be done by expert witness, i.e. a computer forensic investigator. Some countries have added a new section concerning expert opinion on authentication of electronic evidence to their existing laws. India, for example, inserted a new section, i.e. Section 79A of the Information Technology (Amendment) Act 2008, which involves or includes expert opinion as an examiner of electronic evidence. Computer forensic experts have a difficult task to prove the authenticity of electronic evidence, which is to ensure no doubt of any possible alteration during the process of searching, collecting, analysing and presenting the data to the court (Juan, 2011). In *Kennedy v Baker* [2004] FCA 562, Branson said that, "Computer data can be easily altered and merely turning a computer on causes data stored within the computer to change. One of the principal objectives in forensic examination of a computer system is to ensure that data on the computer system is not altered by the examiner during the examination process." In this case, Mr Kennedy sought an order that would prevent the respondents from examining or otherwise dealing with the imaged hard drive and required the delivery up of the imaged hard drive to him. The issue in this case concerns with the extent of the power given to an officer executing a search warrant. The application was dismissed with cost.

A computer forensic investigator is the person most suitable to help establish the authenticity of electronic data. The expert can preserve and ensure from the first step i.e. collection of electronic evidence up to the time when the evidence is produced in court. It means that a computer forensic expert can assist the judicial system in implementing justice relating to the techniques of investigation, i.e. to authenticate electronic evidence (Haneef, 2006).

3. Chain of custody

At the same time, the chain of custody of such evidence is important to ensure that the electronic evidence is authentic and accepted by the court from the time the data were created up to the time they are required (Giova, 2011; Mason, 2010). In *Mohd Ali Jaafar v Public Prosecutor* [1998] 4 MLJ 210 at 229, the appellant was found guilty by the Session court judge. In this case, the learned counsel for the appellant contended that the chain of custody of the tape recordings had not been established by the prosecution. He further said that it must be affirmatively proven and referred to *Ghazali bin Salleh & Anor v PP* [1993] 3 CLJ 638, where Abdul Malik Ishak JC (as he then was) said in p. 644, "since the tape-recorded conversation is susceptible to interference, and can be easily altered, there must be evidence to show that it is well guarded. The essence of any safeguard which is at once real and understandable seems to lie in physically guarding the disc or tape as soon as a recording has been made on it; and making sure that it is

under guard until it is needed for a lawful occasion or until it is brought to the court". Augustine Paul J. said that the authenticity of the recordings had not been proven beyond reasonable doubt as there was a break in the chain of custody. 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 were quashed.

In order to ensure the authenticity of electronic evidence, the expert must be able to show the chain of evidence which will prove the integrity of the evidence before it can be used to support a legal process (Rowlingson, 2004). Furthermore, the investigators need to recognise that the chain of evidence is just as important as electronic evidence as it is with physical types to ensure the integrity of the evidence (Cameron, 2011). Apart from that, the unbroken chain of evidence is also the most effective method to preserving electronic evidence (Group 3, 2014). It can reveal any tampering and error in data entry, which is an evidentiary problem concerning electronic evidence.

It is clear that there are many modes of authenticating electronic evidence such as through testimony of witness, admission, expert opinion and also through the break in the chain of evidence. Electronic evidence is one of the forms of documentary evidence. Documentary evidence is one of the modes of proof other than oral evidence, circumstantial evidence and physical evidence. In *PP v Mohd Abdul Aziz bin Ibrahim* [2013] MLJU 530, although the court admits electronic evidence, they would still fail to prove a prima facie case unless the accused pleaded guilty. This is a murder case under Section 302 of the Penal Code. In *PP v Muhammad Nuzaihan bin Kamal Luddin* [2000] 1 SLR 34, the accused pleaded guilty to unauthorised access to computer materials, unauthorised modification of the contents of a computer and unauthorised access to a computer service under Sections 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] SGHC 33, the accused pleaded guilty for working in syndicate which involved in perpetrating an automated teller machine (ATM) card fraud and was charged under the CMA and the Penal Code. However, if the case is primarily based on the electronic evidence, the court might not be able to convict the accused without any other evidence if there was no weightage or the weightage attached to the electronic evidence is trivial.

CONCLUSION

It can be said that electronic evidence is not synonymous to cybercrime as one might have thought. Electronic evidence also relates to other cases other than cybercrimes; in fact, proof or conviction of the accused is much easier compared to other evidence as electronic evidence is automatically available in hard disks such

as those in speed cameras and in computers. For electronic evidence, however, being a documentary evidence, apart from its clean provenance (i.e., authenticity), legal relevancy and the best evidence rules must be complied in order for it to be admissible. The certificate used for authenticating electronic evidence is not sufficient enough to ensure the originality and genuineness of the electronic evidence or the content. Thus, to ensure that the electronic evidence is authentic, the discovery and preservation of electronic evidence must also be addressed using other evidence. At the same time, the prosecution, through their witnesses, must be able to show that the chain of evidence is unbroken because this will prove the integrity of the evidence before it can be used to support a legal claim. Apart from the modes for authenticating electronic evidence, Malaysia does not have a specific section concerning the authenticity of electronic evidence in respect of the weight to be attached to it compared to Singapore Evidence Act and the US Federal Rules of Evidence. It is proposed that laws on authenticity, reliability, accuracy and their weightage should be made available in the Malaysian Evidence Act 1950 by adopting the Singapore Evidence (Amendment) Act 2012 as a model legislation.

REFERENCES

Adams, C. W. (2011). Spoliation of Electronic Evidence: Sanctions Versus Advocacy. *Michigan Telecommunications and Technology Law Review*, *18*(1), 1–59.

Ahmad, N. (2008). Cryptography, Issues of Privacy and OECD: An Overview. *Current Law Journal*, *9*, liii–lxxxvii.

Armending, T. (2013). *Experts say large-scale security analytics can cut through the noise to find key intelligence. But connecting the dots can lead to legal trouble.* Retrieved June 21, 2015, from http://www.csoonline.com/article/2133455/investigations-forensics/big-data-investigations--opportunity-and-risk.html.

Beal, V. (n.d.). *Big Data*. Retrieved 21 June 2015, from http://www.webopedia.com/TERM/B/big_data.html.

Borisevich, G., Chernyadyeva, N., Frolovich, E., Pastukhov, P., Polyakova, S., Dobrovlyanina, & Losavio, M. M. (2012). 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*, *39*(2), 267–326.

Brenner, S. W. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law & Criminology*, *97*(2), 379–476.

Brenner, S. W., & Goodman, M. D. (2002). *The Need to Harmonize National Penal and Procedural Laws.* International Society for the Reform of Criminal Law, 16th Annual Conference (December 6-10).

Brenton, C. (n.d). Authentication and encryption. Retrieved June 23, 2015, from https://msdn.microsoft.com/en-us/library/cc750036.aspx.

Cameron, S. (2011). Digital Evidence. *FBI Law Enforcement Bulletin*, 14–20.

Chen, Y., Liu, Z., Liu, B., Fu, X., & Zhao, W. (n.d.). Identifying cyber criminals hiding behind wireless routers, 1-14. Retrieved September 24, 2012, from http://www.umac.mo/rectors_office/docs/weizhao_cv/pub_refereed_conferences/2011_conferences/Pkt_Sz_bsd_Traceback.pdf.

Chung, C. S., & Byer, D. J. (1998). The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence. *Boston University Journal of Science & Technology Law*, *4*.

Clancy, T. K. (2011). *Cyber Crime and Digital Evidence: Materials and Cases*. Lexis Nexis.

Gabrys (Ed.). (2002). The International Dimensions of Cyber-Crime, Part 1, *Information Systems Security*, *11*(4), 21-32.

Garfinkel, S. L. (2009). Providing Cryptographic Security and Evidentiary Chain-of –Custody with the Advanced Forensic Format, Library, and Tools. *International Journal of Digital Crime and Forensic*, *1*(1), 1-28.

Garrie, Daniel, B.., &. Gelb, Daniel K,. (2010). E-Discovery in Criminal Cases: A Need for Specific Rules. *Suffolk University Law Review, xliii*(43), 393–416.

Giova, G. (2011). Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. *International Journal of Computer Science and Network Security*, *11*(1), 1–9.

Goodman, M. D. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology*, *10*(3).

Group 3, M. E.-D. W. (2014). IT Technologies and how to Preserve ESI Cost Effectively. *William Mitchell Law Review*, *40*(1), 486–548.

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

Harris, G. J. (2009). Metadata: High-Tech Invisible Ink Legal Considerations. *Mississippi Law Journal*, *78*(4), 939–963.

Kam Wai, W.B. Chik,. (2006). Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore. (Paper) VI Computer Law World Conference, *September 6-8, Edinburgh*.

Keene, S. D. (2012). Financial crime in the virtual world. J*ournal of Money Laundering Control*, *15*(1), 25-37. Emerald Group Publishing Limited 1368-5201. doi: 10.1108/13685201211194718

Kuntze, N., & Rudolph, C. (2011). Secure Digital Chains of Evidence. *Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1-8, Oakland, California, USA, May 26.

Low, W. (2012). Admissibility of Electronic Evidence. *Singapore Law Gazette*, 11-20.

Mason, S. (General Editor). (2011). *Electronic Evidence* (Second Edition). LexisNexis Butterworths.

Maurushat, A. (2010). Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools? *UNSW Law Journal*, *33*(2), 431–473.

Meriam Webster Dictionary (online). Retrieved May 10, 2015, from http://www.merriam-webster.com/dictionary/authentic.

O'Donnell, I. & Milner, C. (2009). *Child Pornography: Crime, Computers and Society*, Devon: Willan Publishing.

Pattenden, R. (2009). Authenticating "Things" in English law: Principles to Adducing Tangible Evidence in Common Law Jury Trials. *The International Journal of Evidence & Proof*, 273-302.

Pollitt, M. M. (2007). The Digital Crime Scene. In J. J. Barbara (Ed.), *Handbook of Digital and Multimedia Forensic Evidence* (pp. 65–76). Totowa, NJ: Humana Press Inc.

Radhakrishna, G. (2009). Legal Issues in Electronic Evidence. *Malayan Law Journal Articles*, *4*(4), 1–11.

Radhakrishna, G., Zan, M., & Khong, D. W. (2013). Computer Evidence in Malaysia: Where are We? Retrieved from http://ssrn.com/abstract=2208973 or http://dx.doi.org/10.2139/ssrn.2208973.

Rockwood, R. (2005). Shifting Burdens and Concealing Electronic Evidence: Discovery in the Digital Era. *Richmond Journal of Law & Technology*, *XII*(4), 1–19.

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness International Journal of Digital Evidence. *International Journal of Digital Evidence*, *2*(3), 1–28.

Ştefan, I. (2011). Cybercrime. *Juridical Current*, *14*(3), 115-120.

Wong, D. H. (2013). Educating for the Future: Teaching Evidence in the Technological Age. *Digital Evidence and Electronic Signature Law Review*, *10*, 16–22.

Wu, X., Zhu, X., Wu, G.-Q., & Ding, W. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*, *26*(1), 97–107. doi:10.1109/TKDE.2013.109.