Volume: 4 Issues: 17 [December, 2019] pp.61-70]
International Journal of Law, Government and Communication
eISSN: 0128-1763
Journal website: www.ijlgc.com

THE INTEGRATION OF DIGITAL FORENSICS SCIENCE AND ISLAMIC EVIDENCE LAWS

Mohamad Khairudin Kallil[1]
Islamic Civilization Academy, Faculty of Social Sciences and Humanities,
Universiti Teknologi Malaysia (UTM), Skudai, Malaysia.
(Email: mkhairudin7@live.utm.my)
Prof Madya Dr. Ahmad Che Yaacob[2]
Islamic Civilization Academy, Faculty of Social Sciences and Humanities,
Universiti Teknologi Malaysia (UTM), Skudai, Malaysia.
(Email: ahmadcy@utm.my)

Received date: *12-10-2019*
Revised date: *20-11-2019*
Accepted date: *24-11-2019*
Published date: *15-12-2019*

To cite this document: Kallil, M. K., & Che Yaacob, A. (2019). The Integration of Digital Forensics Science and Islamic Evidence Laws. *International Journal of Law, Government and Communication*, 4(17), 61-70.
DOI: 10.35631/ijlgc.417006

Abstract: *Evidence is anything that tends to prove or disprove a fact at issue in legal action. It involves the offering of alleged proof through testimony or objects at court proceedings to persuade the trier of fact about an issue in dispute. Islamic Evidence Law is a body of rules that helps to govern conduct and determines what will admissible in certain legal proceedings and trials. In the proceeding that involves digital evidence, the court will consider whether the digital evidence is admissible or inadmissible depends on the requirements of admissibility stated in law statutes in force and the existence of any Standard Operating Procedure (SOP). Under section 33 of the Syariah Court (Federal Territories) Evidence Act or other Syariah Evidence Enactments, digital evidence is subjected to be authenticated by the digital forensics experts. In digital forensics, the process of identification, preservation, collection, analysis, and presentation is the main procedures contained in any Standard Operating Procedure (SOP) of any digital forensics services. The court will ensure that this procedure can maintain the authenticity and the originality of the evidence especially on the issue of expert qualification, a chain of custody and analysis part. Thus, digital forensics is integrated with the Islamic law of evidence to maintain justice in delivering judgment. Therefore, this article examines the standard requirement of the admissibility of digital evidence by digital forensic methodology by using the qualitative approach on the analysis of articles, books, law statutes documents and law cases. The results show that the need for amendment of Syariah Court Evidence and Procedure statutes and the necessity of the existence of Standard Operating Procedure (SOP) on digital evidence in the Syariah courts as a guideline for judges, lawyers and parties involved.*

Keywords: *Digital Forensics, Digital Evidence, Admissibility and Standard Operating Procedure (SOP)*

Introduction

The digital evidence is regarded as primary evidence if the original tools are presenting to the court by recording data or transmitting data. These data will be challenged since the data probably has been modified or edited to be a false document. The need for a procedure under digital forensics science in invalidating the digital evidence is very necessary. Otherwise, the court may reject the evidence because of carrying a suspicious document and doubt. The statutes in force relating to digital evidence under Syariah Court Evidence Act or Enactments are depending on the general requirements provided under admissibility of documentary evidence (al-kitabah), circumstantial evidence (*al-qarinah*) and expert opinion evidence (*al-rakyu al-khabir*). Unlike, under Section 90A of the Malaysian Evidence Act provides the procedure of

authentication by way of giving a certificate of the experts to justify the digital evidence that it is used in ordinary use and working in proper order. Therefore, there must be an effort of amending a new section to the Syariah Court Evidence statutes to establish a Standard Operating Procedure (SOP) of authentication of the digital evidence (Wan Abdul Fattah Wan Ismail, 2016). The suggestion of the procedure that integrated with digital forensics science process is discussed in Allison (2016); F. M. a. Granja (2017) that the authenticity procedures are;

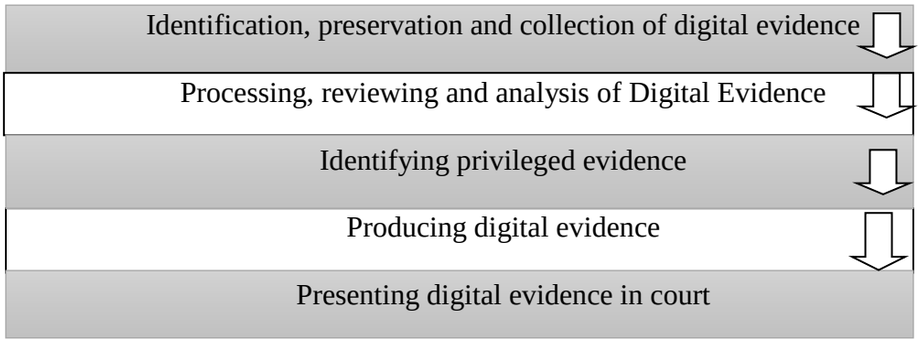

Figure 1: Digital Forensic Methodology

The Syariah Court Evidence Act or Enactments and digital forensics science are so connected to each other to examine and analyses the authenticity of digital evidence presented to the court of law. According to Kiely (2006), science and courts cannot be separated for trial purposes, digital evidence from the testimony of digital forensic experts. The admissibility of the digital evidence is based on the degree of certainty and reliability of the authentication process in digital forensic tools and methodologies (Pieterse, 2017) ;(Antwi-Boasiako, 2017); (Solomon, 2011).

Definition of Digital Evidence

The Syariah Law recognizes digital evidence as documentary evidence and it comes under the definition of "computer"," evidence" and "document" as provided under section 3 of the Syariah Courts Evidence Act (Federal Territories) 1997 (SCEA) or Enactments which states:

> "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.
>
> "evidence" includes all documents produced for the inspection of the Court: such documents are called documentary evidence;
>
> "document" means any matter expressed, described, or howsoever represented, upon any letters substance, material, thing or article, including any matter embodied in a disc, tape, film, sound track or other device whatsoever, by means of-
>
> (a) figures, marks, symbols, signals, signs, or other forms of expression, description, or representation whatsoever;
> (b) any visual recording (whether of still or moving images);
> (c) any sound recording, or any electronic, magnetic, mechanical or other recording whatsoever and howsoever made, or any sounds, electronic impulses, or other data whatsoever;
> (d) a recording, or transmission, over a distance of any matter by any, or any combination, of the means mentioned in paragraph (a), (b) or (c), or by more than one of the means mentioned in paragraphs (a), (b), (c) and (d), intended to be used or which may be used for the purpose of expressing, describing, or howsoever representing, that matter."

The illustration of section 3 provides that matter recorded, stored, processed, retrieved or produced by a computer is a document.

Digital Forensics Science and Digital Evidence

Digital evidence has been defined by the Scientific Working Group on Digital Evidence (https://www.swgde.org/) as information of probative value stored or transmitted in digital form. The records are being stored electronically in digital form (Pollitt, 2006). The term forensic evidence encompasses two distinct ideas and process. The forensics part refers to the laboratory and observational processes utilized in forensics science at an issue through which facts are generated (Kiely, 2006). Digital Forensics science protects digital evidence from possible alterations, damage, data corruption or infection by design or carelessness (Yakubu, 2018). It established procedures for the recovery, preservation and analysis of digital evidence (Britz, 2009). The digital forensics is specifically the more generic area of evidence from all forms of computer activity (Slade, 2004).

Digital forensics evidence can be useful in criminal cases, civil disputes and human resources/employment proceedings (Vacca, 2005). In civil as well as in criminal cases, the parties are seeking to prove or disprove a sufficiently strong connection between the defendant's act or omission and the death or injury in the suit. In both civil and criminal cases, the information provided from scientific sources must be relevant to one of the issues in the case (Kiely, 2006).

Digital Forensics evidence is categorized under real evidence and documentary evidence. However, a complete investigation should address all types of evidence available. The digital evidence will be collected and identified by the forensics examiners in digital forensics procedure (Solomon, 2011). Digital Forensics is the collection of techniques and tools used to find evidence in digital hardware (Caloyannides, 2001).

In obtaining pieces of evidence from the digital tools, the digital forensics procedures must be followed to preserve the originality and authenticity of the evidence. The digital forensics procedures are the collection, preservation, analysis and presentation of digital-related evidence. It takes specialized tools and techniques to collect, examine, analyse and presentation (Pollitt, 2006). Digital forensics can often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted. In other words, the objective in digital forensics is to recover, analyse and present digital-based material in such that it is useable as evidence in a court of law (Vacca, 2005).

In digital forensics, as in any branch of forensic science, the emphasis must be on evidential integrity and security (IPrayudi, 2015). In observing this priority, every forensics practitioner must adhere to stringent guidelines. The forensics practitioner is the digital forensic specialist that the person who responsible for doing digital forensics. The digital forensic specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject digital system (Vacca, 2005).

It is important, therefore to ensure that digital forensics evidence used in information and communications technologies records information accurately and completely (Alhassan, 2018). It is also important that the information or data can be retrieved from the equipment in such a way that its authenticity and veracity cannot be challenged.

Digital Evidence under Islamic Evidence Law

Generally, digital evidence is covered under *al-kitabah* or documentary evidence (Duryana et.al, 2014). Meanwhile, it may come under *al-qarinah* or circumstantial evidence (Ahmad Syukran Baharuddin, 2017). Moreover digital evidence will jointly bring *al-ra'yu al-khabir* (expert opinion evidence) to be involved (Zulfakar Ramli, 2016); (Wan Abdul Fattah Wan Ismail et. al, 2018), whenever the issue of authenticity is challenged in the court of law (Mahmud Saedon A. Othman, 2003).

The Muslim jurists differ to each other to the admissibility of the digital evidence in the court of law. Mahmud Saedon A. Othman (2003) states that the emergence of the various types of documents raises the different views of Muslim scholars to the validity of this evidence. Some

Muslim scholars accept this kind of evidence and it must be considered into account of the judge. However, digital evidence is required to be original and authenticated evidence (Ibn Qayyim, 1977). Other scholars contend that it is not be used as a means of proof as the documents may be forged (Ahmad Fathi Bahansi, 1962).

Digital Evidence under al-Kitabah (Documentary Evidence)

Al-Kitabah is documents, statement or notes written by someone or any types of recording (Mahmud Saedon A. Othman, 2003). The writings or data may be made on official parchment paper and sealed or by transmitting the data into a digital tool like computer or handphone or by snapping pictures in-camera or by recording into video record or CCTV or tape recording. This is supported in Surah Al-Baqarah 2:282 that Allah s.w.t stresses on document writing.

Allah SWT says in the Holy Quran,

يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا تَدَايَنتُم بِدَيْنٍ إِلَىٰ أَجَلٍ مُّسَمًّى فَاكْتُبُوهُ

O ye who believe! When ye deal with each other, in transactions involving future obligations in a fixed period of time, reduce them to writing

In other words, documentary evidence is any evidence introduced at a trial in the form of documents (Nasr Farid Wasil, 1968). Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually includes any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence that provided under several sections for instances section 3, 49, 51 and 56 of Syariah Court Evidence (Federal Territories) Act 1997 or other sections in the Syariah Courts Evidence Enactments.

Digital Evidence under al-Qarinah (Circumstantial Evidence)

Ahmad Fathi Bahansi (1962) defined *qarinah* as together, accompany or related. *Qarinah* also means a thing which explains something. *Qarinah* is actually based on circumstances and surroundings. The authority is derived from Quranic verse in Surah Yusof 12:28, *qarinah* on the Yusof and Zulaikha case. Allah SWT says in the Holy Quran,

فَلَمَّا رَأَىٰ قَمِيصَهُ قُدَّ مِن دُبُرٍ قَالَ إِنَّهُ مِن كَيْدِكُنَّ ۖ إِنَّ كَيْدَكُنَّ عَظِيمٌ

So, when he saw his shirt, - that it was torn at the back, - (her husband) said: "Behold! It is a snare of you women! truly, mighty is your snare!

The circumstances in this situation convey a certain meaning (Nasr Farid Wasil, 1968). It is clear therefore that anything which points to certain meaning, either in the form of words, circumstances, acts or omissions are, therefore, *qarinah* (Wahbah al-Zuhaili, 2004). Thus, digital evidence is regarded as *qarinah* whenever it points and explains about any data that transmitted into a disk or hard disk. It is provided under section 3, 5-16 of Syariah Courts Evidence (Federal Territories) Act 1997 and other sections of Syariah Courts Evidence Enactments. The judge will rely on the evidence and test it whether strong evidence or weak evidence. If there any doubtful, the evidence should be authenticated by calling the opinion of the digital forensics expert.

Digital Evidence under al-Ra'yu al-Khabir (Expert Opinion)

According to Bahansi (1962), *al-ra'yu al-khabir* means the testimony of a person skilled in a certain field or it is the opinion, evidence or testimony given by someone who is skilful in a field or issue. This is highlighted in Surah Al-Nahl:43 that Allah SWT asks to seek experts in any case if the people are unable to answer any problems. Allah SWT says in the Holy Quran,

فَاسْأَلُوا أَهْلَ الذِّكْرِ إِن كُنتُمْ لَا تَعْلَمُونَ

And before thee also the messengers We sent were but men, to whom We granted inspiration: if ye realise this not, ask of those who possess the Message.

A case that participated in digital evidence, the prosecution party must approve that the evidence presented is authenticated. Therefore the court will ask the opinion of those who are proficient or are experts in the chosen field as provided under section 33 of the Syariah Courts Evidence (Federal Territories) Act 1997 and other Syariah Court Evidence Enactments. The opinion given by the expert is based on a high standard of special knowledge (Wan Abdul Fattah Wan Ismail et. al, 2018). The judge who lacks knowledge about the originality of the digital evidence should, therefore, inquire from a person who is skilled in such an issue.

Integration of Digital Forensics Science and Islamic Evidence Law

In obtaining shreds of evidence from the digital tools, the digital forensics procedures must be followed to preserve the originality and authenticity of evidence (F. T. M. Granja, 2017). The digital forensics procedures are the collection, preservation, analysis and presentation of digital-related evidence. It takes specialized tools and techniques to collect, examine, analyse and presentation (Pollitt, 2006). Digital forensics can often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted. In other words, the objective in digital forensics is to recover, analyse and present computer-based material in such that it is useable as evidence in a court of law (Vacca, 2005); (Rago, 2006).

Digital forensics process in Syariah courts can basically be applied with references to the Syariah Courts Evidence (Federal Territories) Act 1997 or Enactments and Civil and Criminal Procedure Codes. The digital forensics methodology will be discussed accordingly as below:

Identification, Preservation and Collection

The first digital forensics procedure above is on the investigation, search and seizure as well subpoena provided by the Syariah court civil or criminal procedure. There is provision found in section 73 (6) Syariah Court Evidence (Perak) Enactment 2004 that the digital evidence shall be admissible in evidence after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

The process of gathering evidence under Syariah Court Civil Procedure (Federal Territories) Act 1998 includes discovery and inspection of documents as well as an interlocutory injunction. The relevant sections in Federal Territories and other states are section 85 for the discovery of documents and facts, section 86 for inspection of documents and section 87 for privileged communications and documents.

The procedures for investigation search and seizure process can be seen in sections 42 to 53 of the Syariah Court Criminal Procedure (Federal Territories) Act 1997 and other Syariah Courts Criminal Procedure Enactments. The related provisions are section 42 for the summons to produce a document or other things, section 55 for the procedure, section 54 for information, section 63 for search by a religious enforcement officer, section 65 for diary of proceedings in an investigation and section 66 for the report of a religious enforcement officer.

Processing, Reviewing and Analysing

The next procedure is analysing the digital evidence by the experts that having a legal valid certificate in digital forensic. In conducting an investigation, there is a plan for the investigation, set up the forensic workstation and install the necessary forensic analysis software to examine the evidence. The type of software to install includes an analysis tool, such as Pro Discover, FTK, and X-Way Forensics (Bill Nelson, 2010). This is noted by Schatz (2007) that the judge will rely on the use of tools and representations by experts as an approach to interpret and assure the digital evidence. The expert must ensure that the digital evidence is working in the ordinary course and working in proper order without any modification (Slade, 2004).

The following procedures are validating step that certified by the digital forensics experts as required by section 33 of the Syariah Court Evidence (Federal Territories) Act 1997 or Enactments state that:

> (1) When the Court has to form an opinion upon a point of foreign law or of science or art, or as to identity or genuineness of handwriting or finger

impressions or relating to determination of nasab, the opinions upon that point of persons specially skilled in that foreign law, science or art, or in questions as to identity or genuineness of handwriting or finger impressions or relating to determination of nasab, are qarinah.
(2) Such persons are called experts.
(3) Two or more experts shall be called to give evidence where possible but if two experts are not available, the evidence of one expert is sufficient. If two experts give different opinions a third expert shall be called to give evidence.

It is supported under section 73 of the Syariah Court Evidence (Perak) Enactment 2004 that:

(1) In any criminal of civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.
(2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.

The requirements of the admissibility the digital evidence under the said section are the digital evidence shall be admissible as evidence, if the document was produced by the computer in the course of its ordinary use, the digital evidence was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who is responsible for the management of the operation of that computer and it shall be presumed that the digital evidence referred to in the certificate was in good working order and was operating properly.

Thus, the court will consider all the requirements and decide accordingly whether digital evidence is admissible or inadmissible in a particular case. The authentication process concerns with the enforcement officers and forensics experts on the identification, preservation and collecting the digital evidence. The forensic experts then, certify that the digital evidence is working and operating in the course of the ordinary used and good working order when conducting digital forensics procedure. The enforcement officer and digital forensics experts must aware of the chain of custody of preservation and analysis process from the scene, transportation, laboratory and software used (Caloyannides, 2001). Meanwhile, the courts also have to approve and recognize the SOP of any digital forensic service like Cyber Security Malaysia (CSM) or other existing digital forensics services (Din, 2012); (Saraswathi, 2019).

Identifying, Producing Privilege Evidence and Presentation of Results of Digital Evidence

Finally, after the process of digital discovery by the experts, they will certify the digital evidence and present the testimony to the court of law. Then, the court has a discretionary power whether to accept or reject the digital evidence based on the weight and high standard of certainty. The rejection of the digital evidence if satisfied that the evidence is tendered is doubtful (Bainbridge, 2008)

According to Kessler (2010) the judges need a general understanding of the underlying technologies and applications from which digital evidence is derived. The judges need additional training in computer and internet technology like the computer forensic process and digital evidence (Wan Abdul Fattah Wan Ismail et. al, 2018). Meanwhile, the consideration is also on the evidence that it has to be collected as early as possible and without any contamination. There must be continuity of evidence, sometimes known as chain custody: that is, it must be possible to account for all that happened to the exhibit between its original collection and its appearance in court, preferably unaltered. All procedures used in the examination should be auditable: that is s suitably qualified independent expert appointed by the other side in a case should be able to track all the investigation carried out by the prosecution experts (Vacca, 2005).

The Framework of Handling Digital Evidence Cases in Syariah Courts

The prior discussion has elaborated the relevant Syariah Laws statutes regarding digital evidence and digital forensics involving digital evidence. The end of this discussion, it results in a framework of handing digital evidence cases in Syariah courts. Figure 2 below shows the proposed framework of digital evidence in Syariah courts.

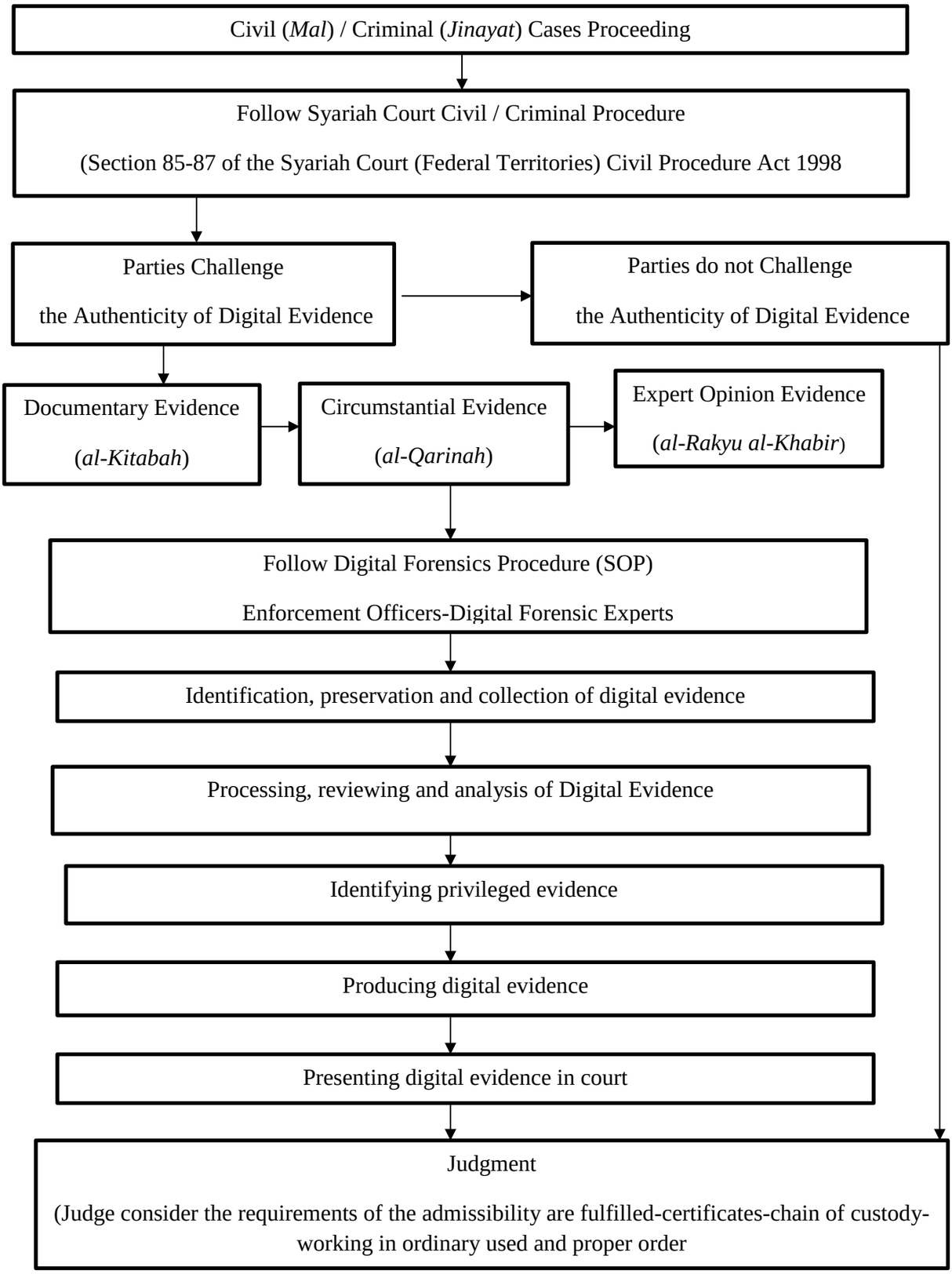

Figure 2: Framework of Digital Evidence Civil (*Mal*) and Criminal (*Jinayat*) Cases

Recommendation and Conclusion

It can be summarized that the integration of digital forensics science and Islamic Evidence Law can be found in the Syariah Court Evidence provision of laws. The relevant sections are concerning on the documentary evidence, circumstantial evidence and expert opinion evidence in Syariah Evidence Act or Enactments and sections under Syariah Courts Civil or Criminal Procedures. However, the exclusive section on the admissibility of digital evidence is not amended yet except Syariah Court Evidence (Perak) Enactment 2004 and the need provision for the enforcement officer to access computerised data as provided in Malaysian Criminal Procedure Code. Thus, the amendment is highly needed.

Besides, even though there are no cases involving digital forensics in a civil and criminal proceeding, the existence of digital evidence can be seen from different digital tools. For example, in the case of *Farah Wahida binti Jamaludin v Adam Kee bin Abdullah*, file case no: (01001-014-0560-2017-JB), the plaintiff Farah Wahida claimed for marriage dissolution (*fasakh*) to the defendant Adam Kee bin Abdullah under section 53 of Johor Islamic Family Enactment (2003). The plaintiff argued that the defendant failed to pay the alimony for several years as well as other responsibilities like home rental cost and nursery payment for the child. Nevertheless, the plaintiff also was abused and injured that causing hurt by the defendant. The plaintiff also said that the defendant was practising Buddha's ritual in a temple. The plaintiff showed the picture of causing hurt and the Buddha ritual picture on that claim. The Plaintiff succeeded in her claim for marriage dissolution (*fasakh*). In the case of *Noor Kamariah Bt Saran v Wan Hashim bin Wan Abdullah*, file case no: (01001-054-1625-2009 - JB), in 18th April 2009, Thursday around 12:34 pm the defendant and the plaintiff had a problem. The defendant had divorced her wife clearly using text messages with three times of divorce as he said in Malay language, *"Macam mana hidup engkau selepas aku cerai dengan talak (3)?*". The plaintiff had referred to the court and the defendant intentionally admitted his word in SMS without any coercion or undue influence and therefore the judge declared officially the plaintiff had been divorced in 3 divorces. In the case of *Pendakwa Syarie Kelantan v Mat Rahim Saman & Satu lagi* ([2004] CLJ (Sya) 513), the accused had been charged under *khalwat* under section 9 (1) & (2) of the Syariah Criminal Code 1985. At the hearing, the accused defended that he possessed marriage certificate (marriage documents) obtained from Thailand authority. The prosecutor asked the judge to examine marriage documents and applied adjournment. However, when hearing resumed, the prosecutor cancelled the examination on the ground that the onus proving was on the accused to authenticate the validity of the documents. The judge held that the accused was not guilty, and the document presented was admissible to the court of laws.

Nevertheless, the decisions of Malaysian Civil Courts cases involving digital evidence are also can be referred to as guidance for Syariah courts in handling digital evidence cases. In order for the digital evidence to be admissible, the party must fulfil the requirements stated in section 90A of the Malaysian Evidence Act. For example, in the case of *Navi & Map Sdn Bhd v Twincie Sdn Bhd & Ors* [2010] MLJU 1210[2011] 7 CLJ 764, The plaintiff produced a certificate ('exh P29') pursuant to s 90A for admission of the printout of the 'Skype chat', duly signed by a digital evidence specialist from the Digital Forensic Department in Cyber Security ('PW4') as evidence for the claim of copyright infringement. Unfortunately, the evidence of the 'Skype chat' did not aid the plaintiff in proving copyright infringement because exh P29 was not a valid certificate under section 90A (2), since it certified that PW4 was not the officer responsible for the management and analysis process of the computer that produced the Skype chats and the certificate did not certify that the document was produced in the course of its ordinary use or that it was in good working order. Meanwhile, the portions of the 'Skype chat' were missing. Therefore, the court held that plaintiff's application against all defendants was dismissed with costs. In the case of *Ahmad Najib v PP* (2007 2 MLJ 505), a murder case that presented digital evidence namely chemist report produced by a computer and a CCTV tape. The chemist was admissible as evidence by the Court of Appeal. The court held that the contents of the chemist report (P83) have the direct effect of linking the appellant to the commission of the offence of murder and rape by him of the deceased. However, a CCTV tape which was considered as a document produced by a computer was inadmissible and had failed to satisfy the requirements of section 90A of the Evidence Act 1950. The appellant (Ahmad Najib) was sentenced to death for the offence under section 302 of the Penal Code and was sentenced to twenty years imprisonment and ordered to be given 20 strokes of the whipping for the offence under section 376 of the Penal Code. His appeal was dismissed by the Court of Appeal.

In short, for the future, if there is arguing or challenging on the authenticity of digital evidence, the digital forensics science can be applied with references to the Syariah and Civil Procedure Act and Enactments as discussed before. Meanwhile, it is suggested that Syariah courts may develop Standard Operating Procedure (SOP) in handling digital evidence cases. The enforcement officer unit may set up the digital forensics unit or the court may approve any SOP from other digital forensic services or agencies like Cyber Security (CSM).

References

Ahmad Fathi Bahansi. (1962). *Nazariyyat al-Ithbat*. Egypt: al-Syarikah al-Arabiah li a- Tibaah.

Ahmad Syukran Baharuddin. (2017). *Di Sebalik Fiqah Forensik*. Selangor: Telaga Biru Sdn. Bhd.

Alhassan, J. K. a. (2018). *Comparative Evaluation Of Mobile Forensic Tools*. Paper presented at the nternational Conference on Information Technology and Systems, ICITS18;, Libertad city; Ecuador.

Allison, R. S. (2016). *The Authentication Of Electronic Evidence.* (PhD), Queensland University Of Technology.

Antwi-Boasiako. (2017). *A Model For Digital Evidence Admissibility Assessment*. Paper presented at the 13th IFIP WG 11.9 International Conference on Digital Forensics.

Bainbridge, D. I. (2008). *Introduction to Information Technology Law* (sixth ed.)

Bill Nelson, A. P. a. C. S. (2010). *Guide To Computer Forensics And Investigations*: Course Technology, Cengage Learning.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime*. London: Pearson Education Ltd.

Buckles, T. (2003). *Laws of Evidence*. New York: Delmar Learning.

Caloyannides, M. A. (2001). *Computer Foensics and Privacy*. Norwood, MA: Artech House.

Din, M. K. B. M. (2012). *Standard Operating Procedure For Digital Evidence in Cyber Crime.* (Master of Computer Science), Universiti Teknologi Malaysia, Malaysia.

Duryana et.al. (2014). Cases Of Electronic Evidence In Malaysian Courts: The Civil And Syariah Perspective. *ICSSR e-Journal of Social Science Research, Vol 1*.

Granja, F. M. a. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics 9*(1), 1-18.

Granja, F. T. M. (2017). Model for digital evidence preservation in criminal research institutions-PREDECI. *International Journal of Electronic Security and Digital Forensics, 9*(2), 150-166.

Ibn Qayyim. (1977). *Al-Turuq Al-Hukmiyyah*. Egypt: Matba'ah Al-Madani.

IPrayudi, Y. a. (2015). Secure And Trusted Environment As A Strategy To Maintain The Integrity And Authenticity Of Digital Evidence. *International Journal of Security and its Applications, Volume 9*(6), 299-314.

Kessler, G. C. (2010). *Judges' Awareness, Understanding, and Application of Digital Evidence.* (PhD), Nova Southeastern University.

Kiely, T. F. (2006). *Forensic Evidence: Science and The Criminal Law* (2nd ed.). Boca Raton, FL: CRC Press Taylor & Francis Group.

Mahmud Saedon A. Othman. (2003). *An Introduction to Islamic Law of Evidence*. Selangor: The Open Press (M) Sdn. Bhd.

Mursilalaili Mustapa Sa'di et. al. (2015). Authentication of electronic evidence in cybercrime cases based on Malaysian laws. *Pertanika Journal of Social Sciences & Humanities, 23*, 153-168.

Nasr Farid Wasil. (1968). *Nazariyyat al-Da'wa Wa al-Ithbat Fi al-Fiqhi al-Islami*. Mesir: Dar al-Shuruq.

Pieterse, H. (2017). *Evaluating The Authenticity Of Smartphone Evidence*. Paper presented at the 13th IFIP WG 11.9 International Conference on Digital Forensics.

Rago, J. T. (2006). *Forensic Science and Law*. London, New York: Taylor & Francis.

Saraswathi, M. (2019). Malaysia's cybersecurity, forensics labs among most advanced in the world. from http://www.bernama.com/en/news.php?id=1730338

Schatz, B. (2007). *Digital Evidence : Reprentation or Assurance.* (PhD), Queensland University of Technology.

Slade, R. M. (2004). *Software Forensics Collecting Evidence From The Scene of a Digital Crime*. New York: McGraw-Hill.

Solomon, M. G. (2011). *Computer Forensics JumpStart* (2nd ed.). Canada: Wiley Publishing Inc.

Vacca, J. R. (2005). *Computer Forensics, Computer Crime Scene Investigation* (D. Pallai Ed.). Hingham, Massachusetts: Charles River Media, Inc.

Wahbah al-Zuhaili. (2004). *al-Fiqhu al-Islami Wa Adillatuh* (Vol. 7). Damsyik: Darul Fikr.

Wan Abdul Fattah Wan Ismail. (2016). Acceptance and Strength of Electronic Documents as Proof in Malaysian Syariah Courts. *Jurnal Undang-undang Malaysia, 28*(2).

Wan Abdul Fattah Wan Ismail et. al. (2018). Evidence Based on CCTV In Criminal Cases An Overview Based On Islamic Law of Evidence. *Malaysian Journal of Syariah and Law, 7*, 87-103.

Yakubu, O. a., Babu, N.C.a, Adjei, O.b. (2018). A Review Of Digital Forensic Challenges In The Internet Of Things (Iot). *International Journal of Mechanical Engineering and Technology, 9*(1), 915-923.

Zulfakar Ramli. (2016). *Aplikasi Undang-undang Keterangan Mahkamah Syariah di Malaysia Dalam Proses Pembuktian Kes Jenayah Syariah di Alam Siber.* Paper presented at the Undang-undang Jenayah Syariah di Alam Siber, Selangor.