UUM JOURNAL OF LEGAL STUDIES
http://e-journal.uum.edu.my/index.php/uumjls

How to cite this article:
Ahmad, M. H., Baharuddin, A. S., Hashim, H., Razak, R., & Saharudin, N. S. (2021). Forensic evidence as a mean of proof in developing prima facie case in takhbib criminal offence. *UUM Journal of Legal Studies*, *13*(1), 221-248. https://doi.org/10.32890/uumjls2021.13.1.10

FORENSIC EVIDENCE AS A MEAN OF PROOF IN DEVELOPING PRIMA FACIE CASE IN TAKHBIB CRIMINAL OFFENCE

[1]Muhammad Hazim Ahmad,
[2]Ahmad Syukran Baharuddin,
[3]Hasnizam Hashim, [4]Ruqayyah Razak
[5]Nurul Syahirah Saharudin & [6]Syaril Nizam Omar

[1,2,3&5]Faculty of Syariah and Law
[6]Faculty of Science and Technology
Universiti Sains Islam Malaysia
Negeri Sembilan, Malaysia
[4]Islamic Science Program, Universiti Sains Islam Malaysia
Negeri Sembilan, Malaysia,
[1,2,3,4&5]Centre of Research for Fiqh Forensics and Judiciary
(CFORSJ) Islamic Science Institute,
Universiti Sains Islam Malaysia,
Negeri Sembilan, Malaysia
[6]Faculty of Science and Technology,
Universiti Sains Islam Malaysia, Malaysia

[2]Corresponding author: ahmadsyukran@usim.edu.my

Received: 23/6/2020 Revised: 25/2/2021 Accepted: 25/4/2021 Published: 31/1/2022

ABSTRACT

A third party's intervention has been one of the most significant factors in Malaysian divorce cases. Third parties may come from

family members and non-family members. This interference is called takhbīb. Within the scope of Malaysian Syariah criminal law, takhbīb is regarded as a criminal offence. However, it is difficult to prove this criminal offence. None of the Syariah law journals reported cases that could be used as reference or case studies. This article proposes a method of proof, which is practical and can be carried out in the Syariah courts to prove the criminal offence of takhbīb. In gathering and compiling the necessary data and related materials, this qualitative study embraced document analysis as a research method. These data are inductively evaluated by implementing qualitative content analysis. This study showed several obstacles in the development of a prima facie prosecution by the Syarie Public Prosecutor, including the absence of eyewitnesses present as evidence. Third-party intrusion is commonly committed through social networks such as WhatsApp, Telegram, WeChat, and Facebook Messenger. The use of such media networks as a medium of contact may also be brought as part of the evidence before the Syariah courts. The best mechanism to be implemented in this case is by using digital forensics and expert opinion. The digital forensic investigator will track or archive the communications from the social media, and deliver them in the form of a written text. In terms of proving the commission of takhbīb criminal offence, this study contributes to the improvement of the Syariah legal system. In short, the law still provides a method of proving criminal offences. Any legal practitioner should make good use of statutory provisions instead of suggesting amendments to it.

Keywords: Fiqh forensics, takhbīb, Syariah court, digital forensic, expert opinion.

INTRODUCTION

According to BERNAMA (2019), third party interference has become the second-highest main cause of divorce among civil marriage with 6,574 cases recorded after the financial problem. In addition, the Department of Islamic Development Malaysia (JAKIM) has identified ten major marital issues, including the intervention of third parties, which compromise the Islamic marital institution in Malaysia (Mohamad et al., 2019). Meanwhile, the research conducted by Shabuddin et al. (2016) elucidated that third-party intervention has

been one of the key causes of divorce between Muslim spouses in Malaysia. These facts indicate the seriousness of the threat of a third party's interference against the marriage institution in Malaysia.

This third-party intervention may come from the family and non-family members (Jusoh & Dimon, 2014). Intervention from the family members may come from father, father-in-law, mother, mother-in-law, sister, sister-in-law, brother, and brother-in-law. Meanwhile, intervention from the non-family members may be committed by close friends, colleagues, ex-lover, ex-fiancé, and secret lover. In short, any person who causes marital disputes is a third party to the marriage. Not only that, a person who intends to interfere for the good sake of the husband and wife in the marital affairs is also considered to be a third party to the marriage (Jusoh & Dimon, 2014).

Based on our observation made in several previous studies like Jusoh and Dimon (2014), Shabuddin et al. (2016), and Ahmad et al. (2019), there were several identified academic gaps, first, lack of scholarly discussion of the *takhbīb* or third-party intervention. Second, the existing intellectual discourses were focusing more on legal reviews and divorce factors. Third, the public was aware of the dangers of *takhbīb* but they do not know how to respond to it. Therefore, this study was conducted to fill in these aforementioned academic gaps. This research will discuss the validity and admissibility of forensic digital evidence in proving *takhbīb*. Furthermore, this study intended to promote and advocate the use of forensic digital evidence by the prosecution in cases related to *takhbīb*.

METHODOLOGY

This qualitative research involved the use of document analysis. This kind of analysis has been recognized as a form of qualitative research (Bowen, 2009, Baharuddin, A.S. et al., 2021), where documents need to be translated and interpreted to get the meaning relevant to the study. Furthermore, the method of analysing the document involves the process of coding into the theme; this process is the same as when analysing the interview transcript (Bowen, 2009; Merriam, 2009). This approach can be executed either as a complementary or stand-alone research methodology (Bowen, 2009; Chinedu & Mohamed,

2017). As for this research, the latter was utilised for appraising the documents written by scholars and academicians.

The types of documents can be primary or secondary. It depends on the source of the document being obtained. If the document is collected afresh for the first time and original, then it is a primary document taken from a primary source. If otherwise, then it is a secondary document (Merriam, 2009; O'leary, 2004). This study has analysed both types of documents. In this study, we appraised three primary documents from the Prophetic traditions which are *Sunan Abu Daud* by Abu Dāud (2009), *Sunan al-Kubra* by al-Nasa'ī (2001), and *Musnad Ahmad* by Aḥmad (2001), *Ṣaḥīḥ Ibnu Ḥibbān* by Ibnu Ḥibbān (1993), and one from Syariah Criminal Offences (Federal Territories) Act 1997 (Act 559). This is because of no clear injunctions provided in the Quranic verses regarding *takhbīb.* The data collected from these primary documents were considered to be the primary data because they came from a direct source, which is reliable and not influenced by any individual view or opinion. Then, the secondary data of this study were the discussions in the classical and contemporary Islamic commentaries and jurisprudence around the theme of *takhbīb*, Islamic criminal law, and Islamic law of evidence. Furthermore, secondary data were obtained from the indexed journals mainly Scopus and WOS related to digital forensic and expert opinion. These documents were obtained from the Scopus database, accessed through the EZproxy portal of the Universiti Sains Islam Malaysia.

The data obtained were then analyzed using Bowen's (2009) preferred document analysis process. This iterative approach incorporates elements of content analysis and thematic analysis (Bowen, 2009). The content analysis method was used to understand, comprehend, and extract meaningful interpretations of data that circulate in the samples and primary documents (Leavy, 2017; Roller & Lavrakas, 2015). In the meantime, thematic analysis was used within the data to identify, analyse, and report patterns (themes) within the data (Castleberry & Nolen, 2018). After the persuasive and significant interpretations have been extracted, the collected primary data was then thematically analysed with the digital forensic and expert opinion published documents. Thematic analysis has been conducted by comparing between the primary data and secondary data to obtain possible and practical means of proving for the commission of *takhbīb*

criminal offense. More focused re-reading and review of the data has been done and relevant coding has been assigned on the data.

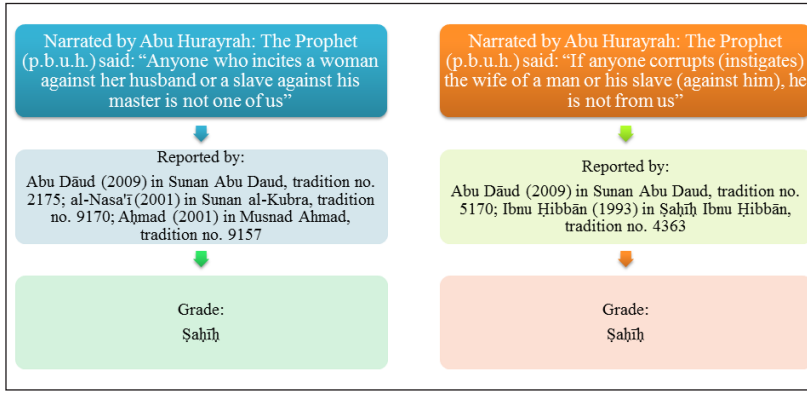
RESULTS

Third-Party Intervention from the Point of View of Syariah

Under Islamic law, interference from the third party to the marriage is considered as *takhbīb*. This term is derived from the word *khab-ba-ba* which refers to beguile (*khadaʿa*), corrupt (*fasād*), malice (*khubth*), and deceives (*ghish*) (al-Fayūmi, 1994; al-Rāzī, 1999; al-Zabīdī, 1987; Ibnu Manzur, 1992). Technically, it means a deceitful man beguiling or corrupting servants or wives to be unfaithful to their master or husband (al-Zabīdī, 1987; Ibnu Manzur, 1992). Meanwhile, al-Zahabi (2003) defines it as an act of beguiling and corrupting a woman's heart against her husband. In a similar vein, Mullā ʿAli al-Qārī (2002) states that *takhbīb* means to beguile or corrupt a wife against her husband by mentioning the husband's faults toward her or all the goodness of another man to her.

Figure 1

Prophetic traditions that prohibit takhbīb (Abu Dāud, 2009; Aḥmad, 2001; al-Nasa'ī, 2001; Ibnu Ḥibbān, 1993)



Perpetrating this act shall be liable of major and destructive sin (al-Zahabi, 2003; Ibnu Hajar al-Haitami, 1987; Ibnu Qayyim al-Jauziyyah,

1997). In addition, Ibnu Qayyim al-Jauziyyah (1997) has explained the prohibition of this act which leads to major sins as follows:

> "...and how many women have been beguiled and corrupted against their husbands, or servants against their masters! Bearing in mind that the Prophet (p.b.u.h.) cursed the one who perpetrates such an act, frees himself from them and declares it to be from the major and destructive sins. Since the Prophet (p.b.u.h.) has forbidden us from as much as proposing to a woman for marriage whilst someone else is in a marriage proposal with her, or out haggling and undercutting his brother in a business transaction,[1] what do you think the severity of exerting effort to separate a husband from his wife or a servant from their master would be?! Yet those who are infatuated with images along with their accomplices do not even see that as a sin. If the infatuated one seeks to reach the one they are infatuated by and also has their own spouse, the matter becomes worse in that it now includes a form of injustice to others that is equal if not more than the sin of lewdness itself..."
>
> (Ibnu Qayyim al-Jauziyyah, 1997, p. 216)

Figure 1 has pointed out two Prophetic traditions that prohibit this heinous act. Syuʿaib al-Arnauṭ in his evaluation of both traditions above has graded them as *ṣaḥīḥ*, have strong transmitted chain, and the narrators were also *ṣaḥīḥ*. According to Ibnu Ruslān (2016) and al-Sindī (2010), whoever perpetrates *takhbīb* is not been considered as a follower of Islam. In addition, al-ʿAzīm Ābādī (1995) and Ibnu ʿIlān (2004) elucidated the act of *takhbīb* refers to the act of a man beguiling or corrupting the wife of another to get a divorce from her husband with the intention to marry her or to marry her with another person. Furthermore, Ibnu Hajar al-Haitami (1987) and Mullā ʿAli al-Qārī (2002) explicated that these traditions apply to husband and wife. This means *takhbīb* is an act of any person who beguiles or corrupts a wife or husband to be separated from his or her spouse.

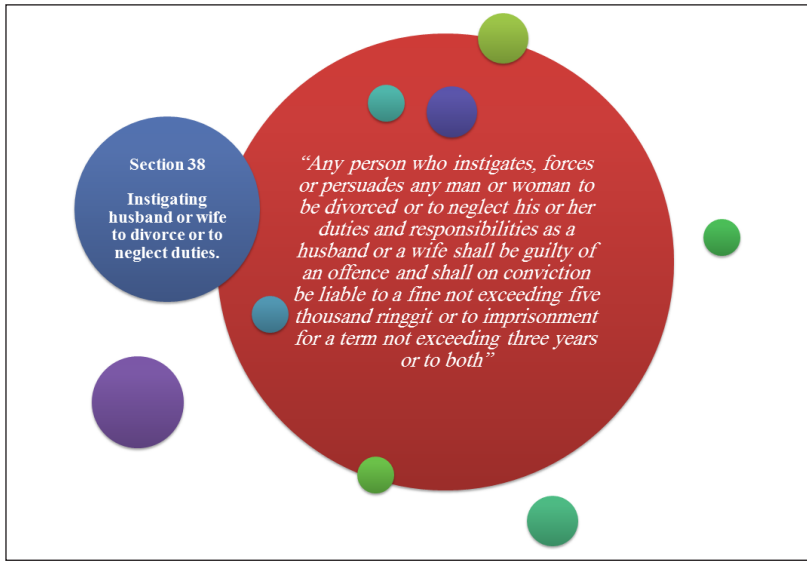
Therefore, based on the abovementioned traditions and their explanations, it can be deduced that *takhbīb* refers to the act of

[1] As reported by Muslim (2016), Prophetic tradition no. 1413, narrated from Abu Hurairah (r.a.).

beguiling or corrupting against wife or husband to become disloyal toward their spouse or instigate them to get divorced from their spouse with the intention to marry them or marry them with another person. This offence is provided under the Malaysian Syariah criminal law in which is evident from Section 38 of Syariah Criminal Offences (Federal Territories) Act 1997 [Act 559][2] quoted in Figure 2.

Figure 2

Section 38 of Syariah Criminal Offences (Federal Territories) Act 1997



On the said provision, it is clearly stated that any person committing *takhbīb* against a wife or husband of the other person shall be liable for the said offence, and punishable with a fine not more than RM5,000

[2] This provision has almost similar essence as the provision of Section 498 in the Penal Code. However, there are some significant differences, among them is that Section 498 is specifically for the husband, where the case will not exist if the husband does not make a complaint to the authorities (Ram & Paul, 2002). Meanwhile, Section 38 is addressed to the husband and wife, and any party may lodge a complaint with the authorities. The second difference is that Section 498 only limits criminal acts against one's wife, while Section 38 includes criminal acts against one's wife or husband. That is, criminal acts committed against any party in a marriage can be convicted.

or imprisonment for not exceeding three years or both (Ismail, 2017). This provision contains two main elements in establishing a case, first, the accused knew or had reason to know that the man or woman is the husband or wife of another person. Second, the accused instigated, forced, or persuaded any man or woman to be divorced or to neglect his or her duties and responsibilities as a husband or a wife. The former shall be *mens rea* while the latter shall be *actus reus*.

Challenges and Difficulties in Proving the Case

The objective of Islamic law of evidence is to formulate principles which are essential for proving facts relevant to the case and aid either to reveal the truth or eliminate the untruth, whether it is extrinsic or intrinsic (Ahmad et al., 2019; Ibnu ʿĀshūr, 2012; Mohamad, 1994; Sayfuddin et al., 1968). There are number of difficulties that arise when Syarie Public Prosecutor intended to establish *prima facie* for *takhbīb* cases. The difficulty includes the availability of eyewitnesses to give testimony in court. The commission of *takhbīb*, particularly the act of instigates, forces, or persuades, is rarely occurred in public. Furthermore, in our modern age which is sophisticated with technology, such acts are easier to be committed online through social media like WhatsApp, Telegram, WeChat, Facebook, and Twitter. The communication is usually done by private messages, email, and phone calls between two persons. In fact, the conversations thread and call logs can also be deleted to avoid being detected by the spouse. These factors have led to the prosecution's difficulty in obtaining eyewitnesses who could see the *takhbīb* act committed by the accused person.

Besides, the prosecutors also confront trouble in proving the elements of the crime stipulated under Section 38 of the Act. Under this provision, as opined by Ismail (2017), the crime is only established when the husband or wife of the other person is proven divorced or neglected their duty as a husband or wife as result from the act of instigates, forces, or persuades committed by the accused person. However, with all due respect, the researchers disagree with this opinion as it is overly stringent and divert from the true meaning and context of the provision. With careful reading on the provision, the law only requires the criminal act of the accused person, which is "*instigates, forces, or persuades any man or woman to be divorced or to neglect his or*

her duties and responsibilities as a husband or a wife". It doesn't require the result from such act either divorce or neglecting duties and responsibilities as husband or wife. Therefore, the researchers believe that it is sufficient to establish the criminal liability if the accused person has committed a criminal act as stipulated in the provision. Apart from that, this provision is established to prevent the destruction of the Muslim marriages. If the law is overly strict with the requirement that divorce or neglect of responsibility is necessary in order to convict the crime, then, it will defeat one of the purposes of Syariah law in Malaysia, to protect the Muslim marriage. In fact, Syariah law in Malaysia will continue to be difficult to implement and fully enforce.

Digital Forensics Investigation Process and Procedures

Third-party intervention is usually achieved by the use of social media such as WhatsApp, Telegram, WeChat, Facebook, and Twitter. As part of the facts, the use of such social media as a means of communication can be brought before the Syariah Court as part of the evidence. In this case, the best mechanism to be implemented is through the implementation of digital forensics.

Previously, it was argued in the case of *Khalid bin Abdul Samad v Ketua Pendakwa Syarie Selangor* (2018) that there is no legal requirement to get analysis and verification from forensic experts upon the digital evidence submitted and presented before the court. In this case, the appellant recommended to the Syarie Judge of Shah Alam Syariah High Court that the video footage marked as exhibit P5 be sent to Digital Forensics Department Cyber Security Malaysia for analysis and verification of its content before it could be admitted by the court. However, the court rejected such a proposal since the appellant failed to establish the legal requirement to do so. In this case, the legal requirement to get analysis and verification from forensic experts can be found by carefully reading the provisions under Syariah Court Evidence (State of Selangor) Enactment 2003, particularly Sections 3, 33(1), 48, 49, and 51.[3] Video footage is part of documentary evidence under Section 3. Section 48 of the

[3] Sections 3, 33(1), 48, 49, and 51 of the Syariah Court Evidence (State of Selangor) Enactment 2003 are *in pari materia* with Sections 3, 33(1), 48, 49, and 51 of Syariah Court Evidence (Federal Territories) Act 1997.

Enactment requires the contents of the document must be proved either by primary or secondary evidence. While Section 51 further provided the document other than written documents to be proved by primary evidence, which means the video footage must be produced and presented for the inspection of the court. However, since Syarie Judge has no skills, experience, and knowledge in dealing with digital evidence, he should seek assistance from the expert opinion to explain it to him. This is provided under section 33(1) of the same Enactment. In the context of digital evidence, Digital Forensics Department Cyber Security Malaysia is the most appropriate expert as this body is an accredited body in dealing with digital evidence. Therefore, such legal requirements are actually present in that case.

Meanwhile, in another Syariah case, *Hisham Halim v Maya Ahmad Fuaad* (2018), the Syariah Court judge accepted the expert opinion given by Mr. Mohammad Zahid Bin Ismail (SD1), an officer from Cyber Security Malaysia who holds the position of Digital Forensic Analyst specializing in digital evidence. He verified the authenticity of a copy of the audio recording (IDD1) which was recorded by the Defendant during her dispute with the Plaintiff. The digital forensic report on IDD1, which was examined by SD1, was submitted to this court. According to him, based on the analysis made as stated in the report, he verified that IDD1 submitted to the court was a copy of the original recording that was made or recorded using the Defendant's mobile phone. The Digital forensic report made by SD1 dated 9/3/2018 was confirmed by Mr. Mohd Zabri Adil Bin Talib, Head of Digital Forensic Department, Cyber Security Malaysia dated 12/3/2018. This report was accepted by the court and marked as D23. In addition, this court also held that the status of SD1 who specializes in the field of digital forensics can be accepted as an expert opinion. This position is in line with the purpose set out in Section 33 of the Syariah Courts (Federal Territories) Evidence Act 1997.

Garfinkel (2010) elucidates that digital forensics traditionally began as an ad hoc and task-oriented practice. This practice was carried out by the computer professionals at that time without formal processes, tools or training. In recent years, digital forensics has developed towards more scientific in the handling of the evidence by enhancing the quality management (Page et al., 2019), error mitigation, tool testing, and verification methodologies (Sunde & Dror, 2019). According to Seigfried-Spellar and Leshney (2016), digital forensics is an umbrella

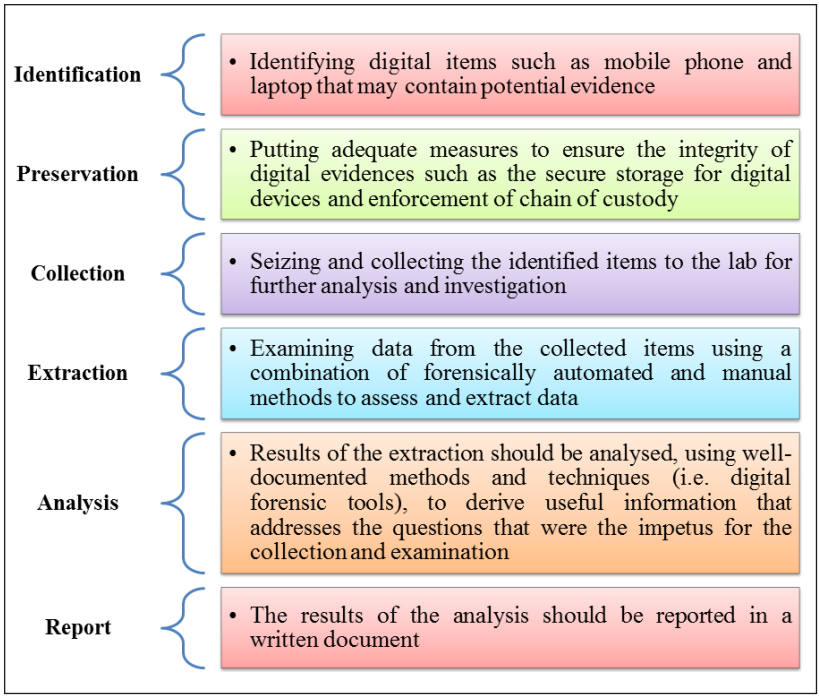
term which refers to digital evidence analysis. This term encapsulates various types of analysing on digital evidences including computer forensics, mobile device forensics, network forensics, and malware forensics.

Brunty and Helenek (2013) elucidates that for cases involving social media, digital evidence is available through the physical device or on the network. As for this study, the focal point shall be on the physical device.

Generally, digital forensics investigation involves a systematic process which can be summarized into six main phases (Johnson, 2014; Pollitt, 2016; Salleh, Mohd, & Khalid, 2014) as illustrates in figure 3.

Figure 3

Digital Forensics Investigation (Johnson, 2014; Pollitt, 2016; Salleh et al., 2014)



Daniel and Daniel (2012) further expounded among the common types of digital evidence submitted before the court are deleted data, internet history, e-mail, social media, cell phones, cellular system and call detail records, and peer-to-peer networks. This statement is closely related to this study as the evidence for *takhbīb* may be submitted in the form of the aforementioned evidence.

Figure 4

Digital Forensic Tools and Their Functions (Cusack & Son, 2012; Mohite, Deshmukh, & Gulve, 2016; MSAB, 2019a, 2019b, 2019c; Murray, 2013; Salleh et al., 2014; Seigfried-Spellar & Leshney, 2016; The Senator Leahy Center for Digital Investigation (LCDI), 2014)

Magnet Internet Evidence Finder (IEF) **Developer: Magnet Forensics**

- Recovers digital evidence from computers, smartphones, and tablets, including both existing cache and deleted data from Internet-related artefacts; chat programs, email, and torrent programs (Murray, 2013; Seigfried-Spellar & Leshney, 2016).
- Magnet IEF also has a special feature called "chat threading," which visually recreates the chat dialog as it would appear on the device (Seigfried-Spellar & Leshney, 2016)

XRY Mobile Forensics Tool **Developer: MSAB**

- Forensically recover deleted data from mobile devices like smart-phones, mobile phones, 3G modems, GPS and Tablet devices (MSAB, 2019a).
- Allows the examiner to communicate with the operating system on the device and request information from the system (MSAB, 2019b).
- Allows the examiner to recover all available raw data stored in the device (MSAB, 2019c).
- Enable the examiner to perform both logical and physical extractions from a device, to recover all the available data from a mobile device, and allowing you to compare the results between the different recovery methods (The Senator Leahy Center for Digital Investigation (LCDI), 2014)

EnCase® **Developer: OpenText Corp**

- Capable of acquiring data from a variety of digital devices, including smartphones/tablets, hard drives, and removable media (Seigfried-Spellar & Leshney, 2016).
- Acquisition, preservation, analysis and presentation of digital evidence (Mohite, Deshmukh, & Gulve, 2016).
- Investigate that require evidentiary data involving Internet usage such as social networking sites, including Facebook and Twitter (Cusack & Son, 2012; Salleh et al., 2014).

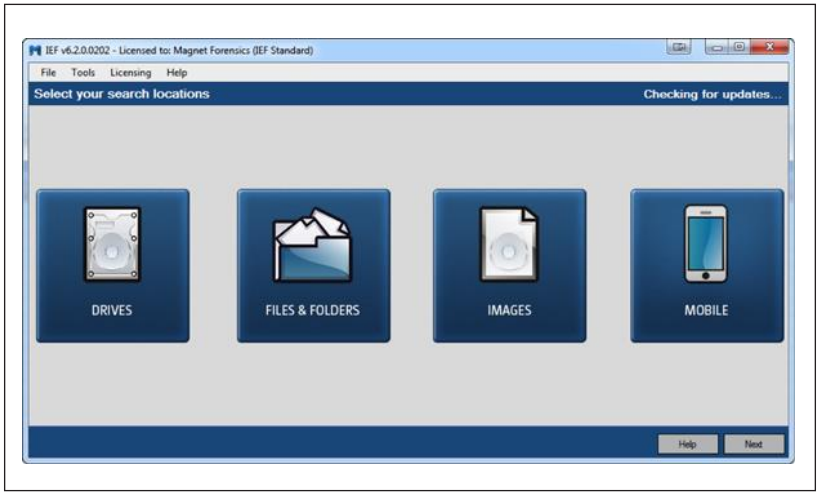
There are several digital forensic tools that can be used to analyse social media artefacts from physical devices. However, the suitability of the tools to be used depends on the type of physical device and operating system to be analysed. There are situations that require only one tool, but there are also some situations that may require several tools to perform a complete extraction. Most forensics investigations on physical devices use commercial digital forensics

software developed for mobile phone forensics investigations such as UFED Physical Analyzer, Magnet Internet Evidence Finder (IEF), XRY, Forensic Tool Kit (FTK®), and EnCase® (Salleh et al., 2014; Seigfried-Spellar & Leshney, 2016). Figure 4 briefly elucidates three tools, Magnet IEF, XRY, and EnCase®, together with their developer and functions. These three digital forensic tools are among the available tools in CyberSecurity Malaysia and the Royal Malaysia Police (PDRM).

These tools can be used to trace or record the conversations through physical evidence seized which are laptop and smartphone. The process of tracing or recording shall be done by the digital forensic examiner. We briefly explained and discussed these three digital forensic tools and their functions in our previous work (Ahmad et al., 2019). In this study, we will focus on Magnet IEF. This tool is among the products developed by Magnet Forensics (Magnet Forensics, 2019b). Generally, Magnet Forensics produces two types of products (Magnet Forensics, 2019a). The first is the lab products that are tools to acquire, analyse, and report on digital evidence and cases. The second product is the agency product to maximize the efficiency of investigative teams.

Figure 5

Magnet IEF software (Williams, 2013)



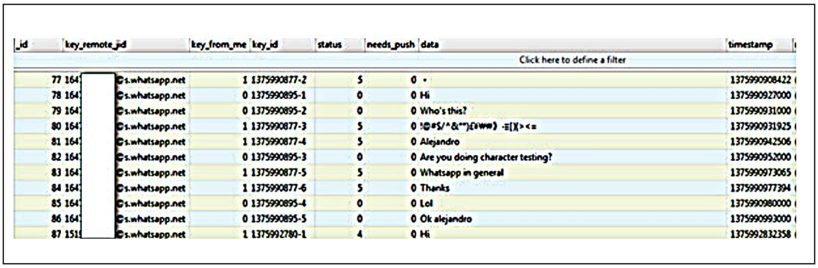
The Magnet IEF is a laboratory product software programme. It is a very common tool that restores digital evidence from computers and electronic gadgets like cache and deleted data from internet-related devices, such as Google Chrome, Mozilla Firefox, and Internet Explorer web browsers; chat-based programs such as WhatsApp, Yahoo Messenger, and Skype; email such as Gmail, Yahoo Mail, and Hotmail; and torrent programs such as eMule, Frostwire, and Ares (Murray, 2013; Seigfried-Spellar & Leshney, 2016). In addition, Magnet IEF has a special "chat threading" mechanism that visually recreates the chat dialog as it appears on the screen (Seigfried-Spellar & Leshney, 2016).

For example, there are key artefacts that should be obtained when investigating WhatsApp. However, it slightly differs between Android and iOS systems. The subject of this research is the Android operating system, where forensic investigators have two useful SQLite databases to recover WhatsApp artefacts, which are msgstore.db and wa.db. Information of every chat dialog between a user and his or her contacts is available in msgstore.db. In the meantime, the wa.db directory saves all contacts of the WhatsApp users.

All of these databases are housed in the database folder and can be located at the following locations:/data/data/com.whatsapp/databases/msgstore.db.and/data/data/com.whatsapp/databases/wa.db. As showed in Figure 6, the msgstore.db database is a very plain SQLite database that consists of a list of chats and messages in tabular form. The message table contains a list of all messages sent or received by the user from his contacts. It includes the contact's phone number, the content of the message sent or received, the status of the message, the time the message was sent or received, and details about the attachments included in the message. Attachments sent through WhatsApp are stored directly in the msgstore.db format. These attachments have their own table entry and there would be a null entry containing a thumbnail and a link to the shared photo/image in the message text. The table can also contain coordinates of latitude and longitude of messages received. This gain would allow the investigator to map out a user's geolocation data.

Figure 6

WhatsApp Messenger Table (Magnet Forensics, 2014)



_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp
						Click here to define a filter	
77	164[redacted]@s.whatsapp.net	1	1375990877-2	5	0	•	1375990908422
78	164[redacted]@s.whatsapp.net	0	1375990895-1	0	0	Hi	1375990927000
79	164[redacted]@s.whatsapp.net	0	1375990895-2	0	0	Who's this?	1375990931000
80	164[redacted]@s.whatsapp.net	1	1375990877-3	5	0	!@#$/^&*")(#W#) -=[]{}><=	1375990931925
81	164[redacted]@s.whatsapp.net	1	1375990877-4	5	0	Alejandro	1375990942506
82	164[redacted]@s.whatsapp.net	0	1375990895-3	0	0	Are you doing character testing?	1375990952000
83	164[redacted]@s.whatsapp.net	1	1375990877-5	5	0	Whatsapp in general	1375990973065
84	164[redacted]@s.whatsapp.net	1	1375990877-6	5	0	Thanks	1375990977394
85	164[redacted]@s.whatsapp.net	0	1375990895-4	0	0	Lol	1375990980000
86	164[redacted]@s.whatsapp.net	0	1375990895-5	0	0	Ok alejandro	1375990993000
87	151[redacted]@s.whatsapp.net	1	1375992780-1	4	0	Hi	1375992832358

A list of all the phone numbers the user has ever contacted is included in the chat_list table. However, the chat_list file does not contain a full list of user contacts. As a result, the prosecutors need to look at the wa.db file. This wa.db file includes a full list of WhatsApp user contacts. This includes the phone number, display name, timestamp, and other details given during WhatsApp registration. In order to acquire access to msgstore.db and wa.db archives, investigators need to root or obtain physical acquisition of Android devices. Alternatively, WhatsApp also maintains a copy of msgstore.db on the SD card used to back up the following locations:/sdcard/WhatsApp/Databases/msgstore.db.crypt. Therefore, an inspection can also be performed from an SD card. One disadvantage of this file is that it must be encrypted and decrypted in order to run the analyses. WhatsApp uses various encryption forms and it depends on the edition of WhatsApp that is used. On the Android operating system, it is reasonably straightforward to recover WhatsApp addresses, texts, and attachments when investigators have access to the required database.

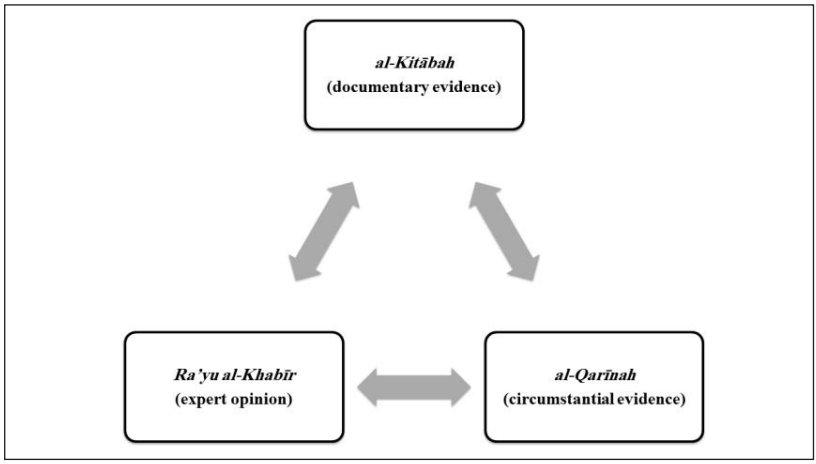
Digital Evidence within Syariah Evidence Law

In essence, digital evidence or digital forensic is closely related to the three types of evidence in Syariah, namely *al-kitābah* (documentary evidence) and *al-qarīnah* (circumstantial evidence) (Baharuddin, 2017a; Kallil & Yaacob, 2019; D. Mohamed & Ramlee, 2014; Sa'di et al., 2014). Meanwhile, digital evidence will involve *ra'yu al-khabīr* (expert opinion) whenever the issue of its validity and admissibility is challenged in court (Othman, 2003; Ramli, 2016; Wan Ismail,

et al., 2018). This is illustrated in Figure 7. These three means of proof are accepted by the jurists in proving a case (al-Zuḥaylī, 1982, 2002; Ahmad M. H. et. al., 2020). In addition, the Syariah Court evidence law in Malaysia also provides for several provisions related to these three types of evidence. This directly shows that digital evidence can be accepted and practiced in the Syariah Court.

Figure 7

Digital Evidence within Syariah Evidence Law



Digital forensic as *qarīnah* can be seen through the existing cache and deleted data from Internet-related artefacts that have been extracted from the physical evidence seized (either smartphone or laptop). These artefacts will be considered as *qarīnah* because they have a relationship or connection with the facts of the case. There may be some who consider that the process of extracting these artefacts from physical evidence is an act that is contrary to laws on privacy and personal data protection. However, it should be noted that in Syariah law, two legal maxims are applied in such situations. The first is "necessity renders prohibited things permissible" (*al-ḍarūrah tubīḥu al-maḥzurāt*). Although the act may be seen as something forbidden, the existence of an exigency has enabled the act. The said exigency is to expose a crime that took place in order to know its perpetrator, and then punishing him. Second, "necessity is determined according to its extent" (*al-ḍarūrah tuqaddaru bi-qadarihā*). This exigency is limited

only to the search for relevant evidence. It cannot go beyond that. If such an act exceeds the limit, then the act is illegal.

Meanwhile, digital forensics as a *kitābah* exists through written reports produced by the forensic examiner. According to Wan Ismail (2020), *kitābah* can be extensively defined as explaining or characterizing something by using writing or sketches or copies that are outward in shape either in the classical forms such as using paper, wood and the like or in modern forms such as the use of diskettes, compact discs, and internet. This definition is not related only to the writings on paper, but also includes media in which information can be stored (Kallil & Yaacob, 2019). It is undeniable that classical jurists hold different views towards *kitābah* as means of proof, however, the majority of the modern legal scholars accept it as a valid means of proof (Arbouna, 1999). With regards to the written reports, among the items to be reported by the forensic examiner may include an explanation of how tools and procedures were selected and a description of the actions conducted (Pollitt, 2016). Chapter 3 of Part II in Syariah Court Evidence (Federal Territories) Act 1997 exclusively provided for dealing with *kitābah*.

Forensic Evidence as Expert Opinion

As explicated earlier, digital forensic evidence will involve experts whenever the issue of validity and admissibility of such evidence is challenged in court (Othman, 2003; Ramli, 2016; Wan Ismail et al., 2018; Wan Ismail et. al., 2021)

The jurists of the four madhhabs have agreed that it is compulsory to refer to experts in matters and things in dispute regarding them before the court (al-Buhūtī, 2003; al-Shirwānī & al-ʿAbbādī, 1983; al-Ṭarābulusi, 2018; Ibnu Farḥūn, 2016). The decision on them depends on the opinion of the experts because they have knowledge and experience that the judge does not know (al-Umar, 2008; Shaniyur, 2005). Furthermore, the jurists are unanimously agreed that the judge must be fair among the litigants because God Almighty says: *"Allah doth command you to render back your trusts to those to whom they are due; and when ye judge between man and man that ye judge with justice."* (al-Quran. al-Nisā' 4: 58). The judge must uphold justice among the disputed parties, and hewill not be able to uphold justice without adequate knowledge on the subject matter from the experts.

Therefore, referring to the expert is deemed compulsory. This is aligned with the Islamic maxims which stated, "*If a mandatory matter is incomplete without another matter, then the other matter also becomes mandatory*." (*mā lā yatimmu al-wājib illa bihi fahuwa wājib*) (al-Umar, 2008; Shaniyur, 2005; Zaydān, 2015).

The opinions of forensic experts are of course relevant to the facts under Section 33(1) of the Syariah Court Evidence (Federal Territories) Act 1997 and may be admissible to furnish the Syariah Court with scientific information related to forensic digital which is likely to be outside the experience and knowledge of a Syarie judge (A. A. A. Mohamed & Nawasdeen, 2005).[4] The Syarie judge may require the attendance of digital forensic examiner to explain their report which

submitted as evidence in Syariah Court. When he received a subpoena to appear in court, he should provide an exhibit that explains how the conclusions were reached (Ahmad et al., 2020). The exhibit should contain a picture or copy of the analysis of the findings. He later should demonstrate in court the use of digital forensic tools that have been applied during the investigation. When giving his testimony, the examiner shall refer to the digital forensic tools presented before the court so that the court can understand the insights and conclusions reached.

Section 33(3) of the same Act further explained that two or more experts are called to testify in Syariah Court. However, if two experts are not available, then evidence from one expert is allowed. Moreover, if the experts called to Court have given different and contradictory opinions, a third expert will be called to give evidence. Based on the opinion of the third expert, the judge will make a comparison and evaluation of the opinions that have been given on an issue, and then the judge will decide whether to accept or reject it.

The Probative Value of Forensic Evidence

Concerning the probative value of forensic evidence, this study agrees with the previous studies stated that it should be *qarīnah al-qāṭiʿah*

[4] However, if a judge can form his own conclusions on the proven facts without any assistance, the opinion of an expert is unnecessary (A. A. A. Mohamed & Nawasdeen, 2005).

(Ahmad, Baharuddin, et al., 2019; Haneef, 2006, 2007; Muhamad et al., 2015; Mutalib & Ismail, 2012). *Qarīnah al-Qāṭiʿah* is defined as convincing circumstances (Haydar, 1991; Sayfuddin et al., 1968), or clear circumstances to a convincing point (Ibnu ʿAbidin, 1992; Ibnu Nujaym, 1997). Although the term used is *"Qarīnah al-Qāṭiʿah*" which means strong or definite *qarinah*, the Islamic jurists refer it only to the level of *ẓan al-ghālib* (beyond reasonable doubt). This is because they find that there are difficulties in any proof including the *qarinah* to reach the level of *yaqīn* (Bak & Ibrahim, 1985; Dabbūr, 1985; ʿUzayzah, 1990). They even consider that no matter how powerful a means of proof, it will never be able to go beyond the level of *ẓan al-ghālib* (Mutalib et al., 2018a). This type of *qarinah* shall stand-alone and does not require any corroborative evidence (Samrūṭ, 2007). Moreover, it is also considered as a conclusive statement (al-Zuḥaylī, 2002).

This study deduced that forensic evidence shall be the *qarīnah al-qāṭiʿah* based on several factors that can be used as justifications for this study. The paramount justification is due to the advanced research development in forensic science and technology. The evidence or exhibits found and collected during the investigation will be analysed using scientific methods. This is done in order to obtain important information that can be used for the purpose of prosecution or claim. This process of analysis is carried out empirically using modern and scientific tools and technologies. The results of the analysis will be obtained in quantitative form as a percentage of the similarity between the analysed exhibit and the suspect.

It is the fact that every general rule comes with exceptions, the same goes for the application of forensic evidence. Forensic evidence shall not be the *qarīnah al-qāṭiʿah* when the evidence fails to meet the prescribed degree of convincing circumstances or clear circumstances to a convincing point. In place of the *qarīnah al-qāṭiʿah*, forensic evidence will be downgraded into *qarīnah ghayr al-qāṭiʿah* which refers to weak or uncertain *qarīnah*. In addition, such *qarīnah* is often used as corroborative evidence to support other evidence (al-Zuḥaylī, 2002; Baharuddin, 2017b). This is due to its nature of not being able to stand on its own and needing support from other stronger evidence (Samrūṭ, 2007). In addition, it is also due to the degree and strength of its proof that does not reach the level of *ẓan al-ghālib*.

In a worse scenario, it can turn into *qarīnah al-kāzibah* where this type of *qarīnah* has no value because it is just a mere presumption or unfounded allegations (al-Zuḥaylī, 2002; Samrūṭ, 2007). Furthermore, Mutalib et al. (2018b) states that sometimes this *qarīnah* has a basis, but it contradicts the stronger *qarīnah*. Conflicts that have occurred have resulted in this *qarīnah* being cancelled directly and cannot be accepted as a method of proof or evidence.

CONCLUSION

In conclusion, the criminal offense of *takhbīb* can be proven through digital forensics. This proposal is made in line with our fully developed era that is filled with cutting-edge technological advances. As of today, offenses are often committed through technological advances such as the crime being discussed in this paper. For that reason, the method of proof of such crimes should also be done by using technological advances. This digital forensic method can be implemented in the Syariah Court because it is closely related to the three types of proof methods in the Syariah Court, namely *al-qarīnah* (circumstantial evidence), *al-kitābah* (documentary evidence), and *raʾyu al-khabīr* (expert opinion). These three types of methods are clearly provided in the evidence law of the Syariah Court in Malaysia. Next, the evidence through this forensic has a high probability value. The paramount justification is due to the advanced research development in forensic science and technology. However, if the forensic evidence used is found to have failed to fulfil the prescribed degree of convincing circumstances or clear circumstances to a convincing point, it will fall to the level of *qarīnah ghayr al-qāṭiʿah* or worse to *qarīnah al-kāzibah*.

ACKNOWLEDGMENT

This work is supported by the Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS) code USIM/FRGS/FSU/055002/50918 (USIM file) - FRGS/1/2018/SSI03/USIM/03/3 (MOHE file).

REFERENCES

Abu Dāud, S. A. A. (2009). *Sunan Abī Dāwud* (S. al-Arnauth & M. Kamil Eds. 1st ed. Vol. 6). Beirut: Dar al-Risalah al-Aliah.

Aḥmad, A. M. (2001). *Musnad al-Imām Aḥmad bin Ḥanbal* (S. al-Arnāwuṭ & Ā. Murshid Eds. 1st ed. Vol. 15). Beirut: Mu'asasah al-Risalah.

Ahmad, M. H., Baharuddin, A. S., Hashim, H., Shah, H. A. R., Ruskam, A., & Harun, M. A. W. (2020). Rejuvenating human capital in Syariah legal institutions through fiqh forensics fundamental module: A preliminary review. *Malaysian Journal of Syariah and Law*, *8*(1), 9-24.

Ahmad, M. H., Baharuddin, A. S., Razak, R., Saharudin, N. S., & Hashim, H. (2019). *Proving Takhbib criminal offense in syariah court through digital forensic evidence and expert opinion.* Paper presented at the 2nd International Conference of the Postgraduate Students and Academics in Syariah and Law (INPAC) 2019, Faculty of Syariah and Law, USIM.

Ahmad, M. H., Baharuddin, A. S., Zakaria, M. A., Nordin, N., Ishak, S. K., & Othaman, N. K. (2020). Bukti saintifik dan penerimaannya di mahkamah syariah: Analisis perundangan bagi undang-undang keterangan mahkamah syariah. *Kanun: Jurnal Undang-undang Malaysia, 32*(1), 67-92.

Ahmad, M. H., Razak, R., Saharudin, N. S., Shah, H. A. R., Hashim, H., Kamaruzaman, N. A. F., Ismail, W. A. F. W., Mutalib, L. A., & Baharuddin, A. S. (2019, 8th-9th October). *Forensic science application towards rahmatan lil alamin: an appraisal within the context of justice.* Paper presented at the 6th International Conference on Quran as Foundation of Civilisation (SWAT 2019), Fakulti Pengajian Quran dan Sunnah (FPQS), Universiti Sains Islam Malaysia (USIM).

al-ʿAzīm Ābādī, M. A. A. (1995). ʿAun al-Maʿbūd Sharḥ Sunan Abī Daud (2nd ed. Vol. 10). Beirut: Dar al-Kutub al-Ilmiah.

al-Buhūtī, M. Y. (2003). *Kashshāf al-Qināʿ ʿan Matan al-Iqnāʿ* (I. A. A. Hamid Ed. Vol. 8). Riyadh: Dar Alim al-Kutub.

al-Fayūmi, A. M. (1994). *al-Miṣbāh al-Munīr fī Gharīb al-Sharh al-Kabīr* (Vol. 2). Beirut: Dar Al-Kutub Al-'Ilmiah.

al-Nasa'ī, A. S. (2001). *al-Sunan al-Kubrā* (H. A. M. Syalbi & S. al-Arnauth Eds. 1st ed. Vol. 8). Beirut: Muasasat al-Risalah.

al-Rāzī, M. A. B. (1999). *Mukhtār al-Ṣiḥḥāḥ* (Y. S. Muhammad Ed. 5th ed.). Beirut: Maktabah al-ʿAṣriyyah.

al-Shirwānī, A. H., & al-ʿAbbādī, A. Q. (1983). *Ḥawāshī al-Shirwānī wa Ibnu Qāsim al-ʿIbadi ʿala Tuḥfah al-Muḥtāj bi-Sharh al-Minhāj* (1st ed. Vol. 7). Egypt: al-Maktabah al-Tijariyah al-Kubra.

al-Sindī, M. A. H. (2010). *Fath al-Wadūd ʿalā Sunan Abī Daud* (M. Z. al-Khawli Ed. 1st ed. Vol. 2). Egypt: Maktabah Liynah.

al-Ṭarābulusi, A. K. (2018). *Muʿīn al-Ḥukkām fīmā Yataraddad Bayna al-Khaṣmain min al-Aḥkām* (O. J. Damiriyyah Ed. 1st ed. Vol. 2). Damascus: Dar al-Qalam.

al-Umar, M. R. (2008). *Uṣūl al-Taḥqīq al-Jinā'ī fī al-Syarīʿah al-Islāmiyyah: Dirāsat al-Fiqhiyyah Muqāranah* (1st ed.). Damascus: Dar al-Nawadir.

al-Zabīdī, M. M. (1987). *Tāj al-ʿUrūs min Jawāhir al-Qāmūs* (A. Al-Hilali Ed. 2nd ed. Vol. 2). Kuwait: Maṭbaʿah Hukumah al-Kuwait.

al-Zahabi, M. A. (2003). *al-Kabā'ir* (A. U. M. H. A. Sulaiman Ed. 2nd ed.). Oman: Maktabah al-Furqan.

al-Zuḥaylī, M. M. (1982). *Wasā'il al-Ithbāt fī al-Sharīʿah al-Islāmiyyah fī al-Muʿāmalāt al-Madaniah wa al-Ahwāl al-Shakhsiyyah*. Damascus: Maktabah Dar Al-Bayan.

al-Zuḥaylī, M. M. (2002). *al-Tanẓīm al-Qaḍā'ī fī al-Fiqh al-Islāmī Dirāsah Muqāranah bayna al-Madhāhib al-Fiqhiyyah wa al-Anẓimah wa al-Qawānīn fī Sūriyah wa al-Saʿūdiyyah wa al-Imārāt al-ʿArabiyyah* (2nd ed.). Damascus: Dar al-Fikr.

Arbouna, M. B. (1999). *Islamic law of evidence: The function of official documents in evidence* (1st ed.). Kuala Lumpur: Syarikat Nurulhas.

Baharuddin, A. S., Abdull Rahim, A., Wan Ismail, W. A. F., Abdul Mutalib, L., & Roslan, S. R. A. (2021). Perkembangan dan pola literatur maqāṣid syarīʿah di Malaysia: Analisis sistematik. (*The development and literature pattern of maqāṣid al-shari'ah in Malaysia: A systematic analysis*). AL-MAQĀṢID *The International Journal of Maqāṣid Studies and Advanced Islamic Research*, *2*(1), 38–55.

Baharuddin, A. S. (2017a). *Di sebalik fiqah forensik*. Kuala Lumpur: Telaga Biru Sdn. Bhd.

Baharuddin, A. S. (2017b). The integration of forensic science fundamentals and Al-Qarinah towards achieving Maqasid Al-Shari'ah. *Doctor of Philosophy. Universiti Teknologi Malaysia, Skudai*.

Baharuddin, A. S., Ismail, W. A. F. W., Johari, F., & Mas'ad, M. A. (2018). A preliminary framework of forensic science fundamentals based on its elements in shariah manuscripts. *Journal of Fatwa Management and Research* (Special Issue) 76-85. https://doi.org/10.33102/jfatwa.vol13no1.155

Baharuddin, A. S., Ahmad, M. H., Ismail, W. A. F. W., Mutalib, L. A., & Harun, M. A. W. (2019). Catalysing global peace through the strengthening of forensic science application in Sharīʿah Law. *Al-Shajarah: Journal of the International Institute of Islamic Thought and Civilization (ISTAC)*, 77-103.

Bak, A. I., & Ibrahim, W. A. A. (1985). Ṭuruq Al-Ithbāt Al-Sharʿiyyah Maʿa Bayān Ikhtilāf Al-Mazāhib Al-Fiqhiyyah Wa Sharĥ Al-Adillat Al-Muwāzanah Bainaha Thumma Muqāranat Bi Al-Qānun Wa Muʿalliqan ʿalaih Bi Ahkām Al-Naqďi. Cairo: Maţbaʿat al-Qāhirah al-Hadīthah.

BERNAMA. (2019). [Infographics] *Divorce cases in Malaysia.* Retrieved on 22 February 2021 from BERNAMA Official Facebook https://www.facebook.com/bernamaofficial/photos/a.10150341276330555/10157523499010555/?type=3&theaterBowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Brunty, J., & Helenek, K. (2013). *Social media investigation for law enforcement* (1st ed.). Waltham: Anderson Publishing.

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10*(6), 807-815. https://doi.org/10.1016/j.cptl.2018.03.019

Chinedu, C. C., & Mohamed, W. A. W. (2017). A document analysis of the visibility of sustainability in TVE teacher education programme: The case of a Malaysian HEI. *Pertanika Journal of Social Sciences and Humanities, 25*, 201-215.

Cusack, B., & Son, J. (2012). *Evidence examination tools for social networks*. Paper presented at the 10th Australian Digital Forensics Conference, Perth.

Dabbūr, A. M. Y. (1985). *al-Qarā'in wa Dauruha fi al-Ithbāt fi al-Fiqh al-Jinā'i al-Islāmi*. Cairo: Dar al-Thaqafah al-'Arabiah.

Daniel, L. E., & Daniel, L. E. (2012). *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom*. Waltham: Syngress.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73. https://doi.org/10.1016/j.diin.2010.05.009

Haneef, S. S. S. (2006). Modern means of proof: Legal basis for its accommodation in Islamic law. *Arab Law Quarterly, 20*(4), 334-364.

Haneef, S. S. S. (2007). Forensic evidence: A comparative analysis of the general position in common law and sharī'ah. *Islamic Studies, 46*(2), 199-216.

Haydar, A. (1991). *Durar al-Hukkām Syarḥ Majallah al-Ahkām* (1st ed. Vol. 4). Beirut: Dar al-Jail.

Hisham Halim v Maya Ahmad Fuaad. (2018). 3 LNS 15 (Syariah Lower Court Federal Territory of Kuala Lumpur).

Ibnu ʻAbidin, M. A. U. (1992). *Radd al-Muḥtār ʿalā al-Dur al-Mukhtār* (2nd ed. Vol. 6). Beirut: Dar al-Fikr.

Ibnu ʿĀshūr, M. Ṭ. (2012). *Maqāṣid al-Sharīʿah al-Islāmiyyah* (5th ed.). Cairo: Dal al-Salam.

Ibnu Farḥūn, I. A. (2016). *Tabsirah al-Ḥukkām fī Usūl al-Aqdiyah wa Manāhij al-Aḥkām* (O. J. Dumairiyyah Ed. 1st ed. Vol. 2). Damascus: Dar al-Qalam.

Ibnu Hajar al-Haitami, A. M. (1987). *al-Zawājir ʿan Iqtirāf al-Kabā'ir* (1st ed. Vol. 2). Damascus: Dar al-Fikr.

Ibnu Ḥibbān, M. Ḥ. (1993). *al-Iḥsān fī Taqrīb Ṣaḥīḥ Ibnu Ḥibbān* (S. al-Arnauṭ Ed. 2nd ed. Vol. 10). Beirut: Mu'asasat al-Risalah.

Ibnu ʿIlān, M. A. M. (2004). *Dalīl al-Fāliḥīn li-Ṭuruq Riyād al-Ṣaliḥīn* (K. M. m. Shihan Ed. 4th ed. Vol. 8). Beirut: Dar al-Maʿrifah.

Ibnu Manzur, M. M. (1992). *Lisān al-ʿArab* (3rd ed. Vol. 2). Beirut: Dar Sadir.

Ibnu Nujaym, Z. I. (1997). *al-Baḥr al-Rā'iq Sharḥ Kanz al-Daqā'iq* (Z. Umairat Ed. 1st ed. Vol. 7). Beirut: Dar al-Kutub Al-'Ilmiah.

Ibnu Qayyim al-Jauziyyah, M. A. B. (1997). *al-Jawāb al-Kāfī liman Sa'ala ʿan al-Dawā' al-Shāfī aw al-Dā'i wa al-Dawā'* (1st ed.). Morocco: Dar al-Maʿrifah.

Ibnu Ruslān, A. H. (2016). *Sharḥ Sunan Abī Daud* (K. al-Ribaṭ Ed. 1st ed. Vol. 16). Egypt: Dar al-Falah.

Ismail, S. Z. (2017). *Undang-undang kesalahan jenayah syariah di Malaysia* (1st ed.). Kuala Lumpur: Penerbit Universiti Malaya.

Ismail, W. A. F. W. (2020). *Keterangan dokumentar menurut Fiqh dan undang-undang keterangan Islam di Malaysia* (1st ed.). Kuala Lumpur: Dewan Bahasa dan Pustaka.

Johnson, L. R. (2014). *Computer incident response and forensics team management: Conducting a successful incident response*. Waltham: Syngress.

Jusoh, Z. Y. M., & Dimon, Z. (2014). *Undang-undang menangani orang ketiga dalam rumahtangga: Satu sorotan dalam undang-undang jenayah syariah negeri Selangor dan undang-undang keluarga sivil.* Paper presented at the International Research Management and Innovation Conference 2014 (IRMIC 2014), Kuala Lumpur.

Kallil, M. K., & Yaacob, A. C. (2019). The integration of digital forensics science and Islamic evidence laws. *International Journal of Law, Government and Communication, 4*(17), 61-70.

Khalid bin Abdul Samad v Ketua Pendakwa Syarie Selangor (2018), 2 ShLR 47 (Shah Alam Syariah High Court).

Leavy, P. (2017). *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. New York: The Guilford Press.

Magnet Forensics. (2014). The rise of mobile chat apps: Recovering evidence from Kik messenger, whatsapp & BBM. https://www.dfir.training/forensic-artifacts/internet/whatsapp/372-magnet-forensics-the-rise-of-mobile-chat-apps-whitepaper-november-2014/file

Magnet Forensics. (2019a). Digital evidence solutions for every step of the case. https://www.magnetforensics.com/products/

Magnet Forensics. (2019b). Magnet's beginning. https://www.magnetforensics.com/our-story/

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation* (2nd ed.). San Francisco: John Wiley & Sons, Inc.

Mohamad, M. N. (1994). Islamic law of evidence in confession (Iqrar): Definitions and conditions. *Islamiyyat-The International Journal of Islamic Studies, 15*, 71-88.

Mohamad, N. Z. A., Malek, N. A., Samsudin, S., & Jani, N. A. (2019). Sustaining the Islamic marriage institution in Malaysia: Lessons from Qur'anic stories. *Al-Shajarah, 24*(1), 97-130.

Mohamed, A. A. A., & Nawasdeen, P. (2005). *The annotated statutes of Malaysia with relevant subsidiary legislation: Syariah court evidence (Federal Territories) Act 1997 (Act 561)*. Selangor: Malayan Law Journal Sdn Bhd.

Mohamed, D., & Ramlee, Z. (2014). Cases of electronic evidence in Malaysian Courts: The civil and syariah perspective. *ICSSR e-Journal of Social Science Research, 1*(2), 1-10.

Mohite, M. P., Deshmukh, J. Y., & Gulve, P. R. (2016). *Qualitative and quantitative analysis of cloud based digital forensic tool*. Paper presented at the 10th International Conference on Intelligent Systems and Control (ISCO) 2016, Coimbatore.

MSAB. (2019a). *XRY - Extract*. https://www.msab.com/products/xry/

MSAB. (2019b). *XRY Logical*. https://www.msab.com/products/xry/xry-logical/

MSAB. (2019c). *XRY Physical*. https://www.msab.com/products/xry/xry-physical/

Muhamad, M. M., Shariff, A. A. M., Rajamanickam, R., Rahman, M. A., Zahid, A., & Ismail, N. (2015). Qarinah: Admissibility of circumstantial evidence in Hudud and Qisas cases. *Mediterranean Journal of Social Sciences, 6*(2), 141-150. https://doi.org/ 10.5901/mjss.2015.v6n2p141

Mullā ʿAli al-Qārī, A. S. M. (2002). *Mirqāt al-Mafātīḥ Sharḥ Mishkāt al-Maṣābīḥ* (1st ed. Vol. 5). Beirut: Dar al-Fikr.

Murray, N. (2013). *Internet Evidence Finder Report*. https://www.champlain.edu/Documents/LCDI/archive/Internet-Evidence-finder-ReportPDF.pdf

Muslim, M. A. H. (2016). *Ṣaḥīḥ muslim* (Y. Hasan, I. Dalli, & I. al-Tiyar Eds. 2 ed.). Damascus: Mu'asasat al-Risalah Nasyhirun.

Mutalib, L. A., & Ismail, W. A. F. W. (2012). Al-Qarīnah: Antara kekuatan dan keperluan dalam mensabitkan jenayah (zina). *International Journal of Islamic Thought, 2*, 1-17. https://doi.org/10.24035/ijit.2.2012.004

Mutalib, L. A., Ismail, W. A. F. W., Mohamed, M. F., Murad, A. H. A., Wafa, K. A. M., & Baharuddin, A. S. (2018a). Al-Qarinah (Circumstantial Evidence) dan peranannya dalam sabitan kes jenayah, munakahat dan kehartaan menurut Islam. In Z. M. Musa, D. I. Supaat, & A. Z. Salleh (Eds.), *Isu-isu Kontemporari syariah & undang-undang* (pp. 97-110). Nilai: Penerbit USIM.

Mutalib, L. A., Ismail, W. A. F. W., Mohamed, M. F., Murad, A. H. A., Wafa, K. A. M., & Baharuddin, A. S. (2018b). Isu-isu dan cabaran sabitan jenayah sihir di Mahkamah Syariah: Satu tinjauan. In Z. M. Musa, D. I. Supaat, & A. Z. Salleh (Eds.), *Isu-isu Kontemporari syariah & undang-undang* (pp. 111-123). Nilai: Penerbit USIM.

O'leary, Z. (2004). *The essential guide to doing research* (1st ed.). London: SAGE Publications Ltd.

Othman, M. S. A. (2003). *An introduction to Islamic law of evidence*. Selangor: The Open Press (M) Sdn. Bhd.

Page, H., Horsman, G., Sarna, A., & Foster, J. (2019). A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? *Science & Justice, 59*(1), 83-92. https://doi.org/10.1016/j.scijus.2018.09.006

Pollitt, M. (2016). The key to forensic success: examination planning is a key determinant of efficient and effective digital forensics. In J. Sammons (Ed.), *Digital Forensics: Threatscape and Best Practices* (pp. 27-43). Waltham: Syngress.

Ram, G. S., & Paul, A. (2002). *Mallal's penal law*. Kuala Lumpur: Malayan Law Journal Sdn Bhd.

Ramli, Z. (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, Alam Siber, Selangor.

Roller, M. R., & Lavrakas, P. J. (2015). *Applied qualitative research design: A total quality framework approach.* New York: The Guilford Press.

Sa'di, M. M., Kamarudin, A. R., & Ramli, Z. (2014). Reception of electronic evidence from Islamic perspective. *Australian Journal of Basic and Applied Sciences, 9*(26), 30-35.

Salleh, R. M., Mohd, M., & Khalid, K. B. (2014). Validation of digital forensics tools for android tablet. *Journal of Information Assurance and Security, 9*, 19-26.

Samrūṭ, W. A. (2007). *al-Qarīnah Wa-Atharuhā fī Ithbāt al-Jarīmah: Dirāsah Fiqhiyyah Muqāranah* (1st ed.). Beirut: Manshurāt al-Halabi al-Huqūqiyyah.

Sayfuddin, Khalīl, A. S., Jūdat, A., Khalid, A., al-Ḥilmī, A. S. A., Khuluṣī, A. S. A., Satār, A, & Ḥilmī, U. (1968). *Majallah al-Aḥkām al-ʿAdliyyah* (5th ed.). Beirut: Matbaʿah Shaʿariku.

Seigfried-Spellar, K. C., & Leshney, S. C. (2016). The intersection between social media, crime, and digital forensics: #WhoDunIt? In J. Sammons (Ed.), *Digital Forensics: Threatscape and Best Practices* (pp. 59-67). Waltham: Syngress.

Shabuddin, N. S., Johari, N., Abdullah, N., & Aziz, S. (2016). Perceraian dalam kalangan pasangan dewasa pertengahan di pejabat agama Islam daerah Hulu Langat (PAIDHL): eksplorasi faktor. *Jurnal Sains Sosial, 1*, 36-52.

Shaniyur, A. N. M. (2005). *al-Ithbāt bil-Khibrah bayna al-Qaḍā' al-Islāmī wa al-Qānūn al-Duwali wa Taṭbiqātihā al-Muʿāṣirah: Dirāsah Muqāranah* (1st ed.). Oman: Dar al-Nafa'is.

Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation, 29*, 101-108. https://doi.org/10.1016/j.diin.2019.03.011

The Senator Leahy Center for Digital Investigation (LCDI). (2014). *XRY Tutorial: Logical Extraction of Data from Windows OS Devices*. The Senator Leahy Center for Digital Investigation (LCDI):https://www.champlain.edu/Documents/LCDI/Windows_OS_Tutorial_Final_PDF.pdf_

ʿUzayzah, A. H. (1990). *Ḥujjiyyah al-Qarāin fī al-Sharī'ah al-Islāmiyyah: al-Baṣm āt, al-Qiyāfat, Dilālat al-Āthār Taḥlīl al-Damm*. Oman: Dār ʻAmmār li al-Nashr wa al-Tawzī'.

Wan Ismail, W. A. F., Shukor, S. A., Hashim, H., & Baharuddin, A. S. (2018). Pembuktian melalui televisyen/kamera litar tertutup (CCTV) dalam kes-kes jenayah: Tinjauan umum berdasarkan undang-undang keterangan Islam. *Malaysian Journal of Syariah and Law, 7*(1), 87-103.

Wan Ismail, W. A. F., Hashim, H., Mamat, Z., Abdul Mutalib, L., Baharuddin, A. S., & Jusof, N. (2021). Sumpah Nafy Al-'Ilmi menurut undang-undang keterangan Islam di Malaysia. *Nafy Al-'Ilmi Oath According to Islamic Law of Evidence in Malaysia*. AL-MAQĀṢID *The International Journal of Maqāṣid Studies and Advanced Islamic Research*, *2*(2), 25–37.

Williams, S. (2013, 25th October). Magnet forensics – free tool: IEF logical evidence file creator for encase v7. https://www.forensicfocus.com/News/article/sid=2108/

Zaydān, A. K. (2015). *al-Wajīz fī Sharḥ al-Qawāʿid al-Fiqhiyyah fī al-Sharīʿah al-Islāmiyyah* (1st ed.). Beirut: Muasasat al-Risalah Nasyirun.