A Legislative Analysis of Malaysian Legal System on Search and Seizure Procedure of Digital Evidence

Zainal Amin Ayub[1] Mohamad Fateh Labanieh[2] Harlida Abdul Wahab[3]

[1]Universiti Utara Malaysia, Malaysia
[2]Universiti Utara Malaysia, Malaysia
[3]Universiti Utara Malaysia, Malaysia
m.fateh.labanieh@uum.edu.my

Abstract. Nowadays criminals use computers to commit various crimes both in the virtual and real world. These activities store digital evidence which can be used in criminal proceedings. The advancement has led to the searches and seizures of digital evidence. The legal framework of obtaining digital evidence needs to cope with the advancement of the digital era. Being a Commonwealth country inheriting a common law system, this article aims to assess the adequacy of the laws on searching a person's property and confiscation of any digital evidence in Malaysia, with comparison to the laws in England and Wales. The article adopts the qualitative research design, analysing the legal system of Malaysia. It is found that the laws in Malaysia have not adequately been revised following the advancement in technology on search and seizure procedures in the digital era. The professionals are still pursuing to overcome cybercrime activities. On the contrary, the laws of England and Wales have been more comprehensive in this context. The existing laws should be amended according to the experience learnt from England and Wales. Future research can retest the research questions based on the legislative analysis of the Malaysian legal system on the search & seizure procedure of digital evidence.

Keywords: Cybercrime; Digital Evidence; Malaysian Legal System; Search and Seizure

1 Introduction

In the field of technical infrastructure, the internet has proved to be the fastest-growing area of development. The trends towards digitization are increasing with time while demand for computers and internet connectivity has led the technology of computers to higher levels [1]. The initiation of digital evidence has turned out to be dreary as people and individuals retort to justifiable business dealings. The pre-dominance of maltreatment has focused concentration on the expansion of systems to counter computer-generated transgressions and cyber interfering. Digital evidence is any information of a verifying nature that is stored, sent out, or recovered in binary form [2]. The progression of the digital universe puts forward enormous amounts of information flow and data

R. Abdul Rahman et al. (eds.), *Proceedings of the 12th UUM International Legal Conference 2023 (UUMILC 2023)*, Atlantis Highlights in Social Sciences, Education and Humanities 15,
https://doi.org/10.2991/978-94-6463-352-8_20

transmission, thus creating an abundance of digital evidence. International Data Corporation (IDC) reported that the total amount of digitalized data in 2007 was 281 exabytes (one exabyte is equal to a billion gigabytes) and the amount would reach close to 1800 exabytes in 2011 [3]. Meanwhile, EMC Digital Universe estimates that the amount of data produced in the year 2020 will increase to 44 trillion gigabytes [4]. These bytes may become digital evidence in any criminal case.

To find digital evidence of the crimes, the modernization of computers has led to the searches and seizures of data, which are stored on the computers' hard drives or any equivalent storage system. The concept of the latest "search and seizure of digital evidence", has, therefore, been introduced by this technology. The criminal justice system of Malaysia has provisions to facilitate such search and seizure of digital evidence. The focus of the study was the practice and position of search and seizure law in Malaysia. It further aimed to discuss the potential and critique reforms as implemented in England and Wales [5] [6]. The adequacy or compatibility of the existing laws is addressed to examine the sufficiency of legal powers, or powers that have been approved but might be inappropriate in the scope. The compatibility and adequacy of the laws are important as it affects the effectiveness and fairness during procedures of the search and seizure of digital evidence [7].

2 Methodology

The practices of cybercrime have become the main risk in Malaysia to the private and public sectors since it is planned to move the majority of the operations using a submission through automated communications. This has made the work to be well-organized and effectual, but risks produce a set of troubles, and a majority of the time the automated pressures produce economic achievements [8]. The qualitative research design has been implemented to evaluate the legislative analysis of the Malaysian legal system relating emerging search and seizure procedure of digital evidence. The research will benefit from a comparative analysis of relevant Malaysian legal provisions with that of England and Wales. To make the proper comparison, all the published articles considering the qualitative approach have been selected for the study.

Most appropriate studies have been preferred for collecting the data. The abstracts, theses, and unpublished articles which were assembled in duplicate studies were excluded immediately. The standard guidelines were used for developing the qualitative analysis of the survey. The qualitative review has been collected and data has been analysed from the selected studies in agreement with the objective.

The qualitative analysis has extracted the data from the authentic studies to obtain the appropriate data. The abstract was screened to obtain suitable studies. Furthermore, a complete study was done for assessing the quality of data with the authenticity of selected resources. The procedure was strictly monitored to get the most appropriate and authentic research articles to develop the qualitative analysis. The interventions, which have been used in the review were related to the Malaysian legal system on the proposed issue and then some comparison with the similar legal provisions of England and Wales. The research articles that have been selected for the review have shown interventions to evaluate the legislative analysis of the Malaysian legal system on the search & seizure procedure of digital evidence.

3 Digital Era - Digitisation Of Evidence

The digital era or the computer and the digital environment have offered new opportunities to criminals to engage in various types of online and offline crimes. What it means among other things is that criminal activities using digital means will store digital evidence in the same device criminals use for committing the crimes. While they create new online crimes termed cybercrimes like hacking, they also facilitate the commission of offline, traditional, or customary crimes like fraud. The widespread use of computers and digital devices has also led to searches of data stored on hard drives and other storage devices.

Cybercrime or any other computer-related crime is an offense covered by illegal deeds, by way of a computer system or network [9]. It originates damage or loss to the tools, information, and data that occupies the processing or software of the computer. It may be due to a virus attack, unauthorized access, and use, or data theft on an electronic device that becomes the objective of cybercrime [10] [11].

Search and seizure are some of the very important procedures that mostly occur during any investigation of crime. In this information age or digital era, the proliferation of computer and information technology generates an abundance of digital evidence in digital devices [12]. According to an IDC report in 2014, 14 billion devices are communicating through the Internet nowadays and another 200 billion digital devices are connected to the Internet [4]. Again, these digital devices may store or contain digital evidence and as such will always become an object of search and seizure in any criminal investigation.

3.1 The Rise of Cybercrime

A very broad range of criminal activities are included in cybercrimes and a majority of these crimes are committed in the real world. Since the concept is very new, relevant authorities, like the police, public agencies, and the business world are yet to agree on a comprehensive definition for cybercrime. The cyber-world or the world of modern information technology has become an avenue for a variety of crimes committed through the computer or the internet.

Malaysia is one of the most appealing countries in Asia in cybercrime activities. The total number of internet users was 28 million in the year 2020, an increase to 88.7 percent [13]. The extensive practice of the internet is opening chances by making it susceptible to cybercrimes. The platform for cybercrime has been provided by the nature of the internet itself to perform unlawful actions from anywhere in the world. According to the Norton Cybercrime Report 2010, up to 83% of internet users in Malaysia have been a victim of cybercrimes [14] but it was decreased to 49% of internet users experienced cybercrimes, especially fraud in 2020 [13]. According to Computer Crimes Act, the Multimedia Act and Communications' and the Panel Code, hacking has mainly governed the cybercrimes [15]. The misuse of the computer can be considered to cover the situations in which the computer or IT-related properties are abused. This could comprise mainly novel crimes, which are directly ensured from IT development such as illegal access, rejection of service attacks, and so on.

Fraud and computer misuse are the most ordinary online crimes reported by the Crime Survey for England and Wales (CSEW) under the Office for National Statistics (ONS), where there are 2956 incidents reported in 2018 [16]. The CSEW presented a somewhat diverse tendency, which has shown an augmentation in the likelihood of being a fraud and computer misuse victim, ten times more likely than being a victim of theft and 35 times more likely than being the victim of a robbery [17]. The number of mature users of the internet, practicing PC viruses is observed to have reduced, since the mid of the 2000s [18]. Similarly, the usage of the software that limits tracking of activities also decreases to only 27% among mature users. Data extracted from the ONS illustrates that the number of internet users who do not have smartphone security software decreased from 26% in 2018 to 17% in 2020 [19], indicating the number of internet users who are concerned about their online security has increased steadily.

Regarding e-commerce, the victim surveys suggested that approximately 10% of the users of the internet have taken something online, from where the information was misused. It has been suggested that many organized cybercriminals do not operate in the traditional manner. They do many efforts as loser networks of pre-arranged cybercriminals as part of the worldwide online market. They could easily sell and buy the technological tools or products derived from, or services used for, attacks of cybercrimes [20]. These teams have been working in a pre-arranged structure, but different from the usually organized crime authorities. The persons in the online environments, are not restricted by the similar domination and hierarchy and be inclined to effort mutually as a movable association for a limited and shorter time interval, rather than on a long-lasting source [21] [22].

4 Digital Era – The Challenge

In Malaysia, there have been many fraud cases related to cybercrimes reported throughout the last few years, but no sufficient executive approximations have been designed by any governmental body or authorities. There is a need for studies to be performed on cybercrimes, and traditional crimes facilitated by the internet such as frauds, as well as on the Malaysian legal system on search and seizure procedure of digital evidence, with some comparison made with England and Wales. Specifically, it has been determined by the customs of the country that seems apparent in arguing these problems in detail within the government activities, academics in general, and private practices or regarding the works done by Transparency International Corruption Perception Index (TICPI) 2007-11 [23].

One example of the issues that have been recognized concerning the online fraud crime by the scammers, where the situations like these are endlessly reported to be rising. The misuse of student pass has been a major problem. Further investigations explored that, the scammers are mistreating their student visas to enter Malaysia and are deliberately involved in online crimes. Some students from Nigeria, living in Malaysia, were not authentic students according to the consul-general at the United States Embassy. As per the Education Ministry, there are 9,146 students out of 123,000 total students from overseas [24]. The scammers have oppressed the drive of Malaysia to be a worldwide hub by protecting the visas of students to attend universities. The policy has been persuaded by Malaysia to attract international students, allowing a great number of foreign colleges to set up campuses in Malaysia [25].

In Malaysia, there were initiatives taken by audit firms to reveal some judgments for fraud, generally for commerce. The techniques were not as convincing as they should have been to signify the reasons behind such frauds. According to the audit survey done by Klynveld Peat Marwick Goerdeler (KPMG) on the Fraud Survey Report, Global Economic Crime Survey (GECS) by industry and Price Waterhouse Coopers (PWC), the data collection within suitable ranges was due to the positive restrictions of the participants [26]. The study has examined some cases of cybercrimes that happened in Malaysia and drawn it into a variety of theories. The cases of cybercrimes expanded and kept rising not just in Malaysia, but all around the globe [25]. Some of the principles cover search and seizure responsibility to oblige with the survey authorities and the use of international and encryption collaboration [27].

The rising figure of cases comprises digital evidence, which includes emails. Digital evidence affects every facet of law, including civil and criminal laws. The digital evidence is significantly relevant in Malaysia as well as in England and Wales as the World Wide Web and Internet have become ever-present technology. The Public and Commercial organizations both depend on the technological environment that has become a major part of their survival and business [28]. When the organizations use the internet facilities and emails, they will also have to become well-aware of the digital evidence. Malaysian lawyers must start understanding the technical issues that are related to digital evidence [29] [30].

5 The Law on Search and Seizure of Digital Evidence

Some states have evaluated their domestic criminal laws to conclude if it is sufficient to combat the new phenomenon to assemble the disputes created by cybercrime. Consequently, some countries have already altered their laws, which include countries like the United States, Greece, Denmark, France, Australia, and Switzerland. Malaysia and Singapore have endorsed legislation to stop cybercrimes that are related to computer according to the Computer Crimes Act 1997. The Act covers four crimes: illegal admittance with the aim to assist the commission of additional offences, illegal adjustments in the data of computers, and wrong contact with the unlawful web. It also criminalizes assisting, supporting, and attempting to commit any of these crimes. In the legal field, when the information is preserved through the devices, it is important to keep and maintain it for a time until the investigation has been done.

Malaysia has always been trying to be at the forefront of the development of technology. The Internet has turned out to be a necessity in business, communication, socialization, and many others. There are, however, a number of reckless people that are using the networks through illegal ways, which includes identity frauds and web love scams, regardless of being an optimistic instrument for consumers. Consequently, the government of Malaysia has already taken steps to conquer these problems by commencing numerous acts of law to deal with the issues of cybercrimes. According to the list of acts in Malaysia concerning cyberlaw, there should be a regular review and updates of the current internet crimes in Malaysia as the technology of information has evolved swiftly in recent years [31]. Computer Crimes Act 1997, Communications and Multimedia Act 1998, Digital Signature Act 1997, Copyright Act (Amendment) 1997, Electronic Commerce Act 2006, Electronic Government Activities Act 2007, Personal Data Protection Act 2010, Payment Systems Act 2003, Telemedicine Act 1997, Penal Code, and Multimedia and Communication Content Code are commonly implied legislative acts in against of cybercrime [32]. Applicability and relevancy of the criminal laws, which are related to cybercrimes are also need to be aligned, just for making sure the legislation is complied with.

Regarding the procedures, the Criminal Procedure Code is the main legislation to govern the procedural aspect of criminal investigations in Malaysia. To cope with the advancement of the digital era, Malaysia also introduced new provisions to govern the search and seizure of digital evidence in 2012. Due to the lack of any provision that specifically deals with search and seizure of digital evidence, the Parliament of Malaysia passed a new provision, that is section 116B of the Criminal Procedure Code, to deal with this matter. Along with the introduction of section 116B, sections 116A and 116C are also introduced [30].

Section 116 generally provides for the powers of search and seizure of the police. The section also relates to the summons for production issued under section 51 of the Code. Section 116A further enhanced the power of search without any warrant. The search and seizure without warrant give the police the powers to take possession of any book, document, record, account or data, or another article; or inspect, make copies of, or take extracts of the book, document, record, account, or data, or other article seized. The word "data" here refers to any data held on a computer or any digital device.

Section 116B then specifically refers to the search and seizure of digital evidence where it provides for the power to access computerised data. The said section 116B is reproduced here and reads: -

"(1) A police officer not below the rank of Inspector conducting a search under this Code shall be given access to computerized data whether stored in a computer or otherwise.

(2) Any information obtained under subsection (1) shall be admissible in evidence notwithstanding any other provisions in any written law to the contrary.

(3) For the purpose of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data."

5.1 The Law on Search and Seizure of Digital Evidence – Adequate and Effective?

While the intention of the introduction of sections 116A, 116B, and 116C are to cope with the advancement of digital evidence in the digital universe era and make the life of investigators a little bit easier but are they adequate and effective?

Before the introduction of sections 116A, 116B, and 116C of the CPC, the main governing provisions on the search and seizure procedure of digital evidence in Malaysia are the same provisions that govern the search and seizure of tangible or physical evidence. It is argued that digital evidence is different in its nature as compared to physical evidence. It is 'fragile'[33] as it is easily altered and modified without a trace. Hence, the search and seizure procedure of the evidence must cope with the 'fragile' and different nature of digital evidence. Indeed, the types of digital evidence may differ with the different types of crimes involved. As such, the move to introduce sections 116A, 116B, and 116C by the Parliament is lauded. The said sections were introduced via Criminal Procedure Code (Amendment) (No. 2) Act 2012 (Act A1431) Section 4 and in force from 31 July 2012.

Subsection (2) clearly "legitimises" the computerised data or digital evidence obtained even if the evidence seized is contrary to any other provisions or any other laws. The "access" must be given to the police and includes being provided with the necessary password, encryption code, decryption code, software or hardware, and any other means required to enable comprehension of the computerized data. The trio of sections is summed up with section 116C which provides for the power of interception of communication, installing the interception devices as well as the power to compel the Internet or the communication service provider to intercept and disclose the communication.

The provision under subsection (3) of section 116B provides for the power of the police to compel the person to give the password, encryption, and decryption code, to enable the comprehension of the computerised data and to require that information in the computer be made accessible to be produced and taken away in a visible and legible form. The provision may be used to compel the production of an encryption key. Any refusal or non-cooperation with the requirement of enforcement officers will amount to obstruction of justice and make the individual who fails to co-operate will be subjected to a criminal charge. However, to say that these provisions are effective, where there are a requirement under the law to give up the encryption keys, is very hard to enforce in practice because there is no reported case on obstruction of justice for denying the requirement to give up an encryption key. Hence, dependent upon the circumstances of the case, the provision may be ineffective (i.e. criminalising people for not giving up the encryption key) because the individual chose not to reveal the encryption key. After all, the punishment would be greater if the real offence were revealed.

Based on the provisions above, the provisions emphasise the power of search and seizure of digital evidence and its admissibility notwithstanding if the contrary occurs during the procedures. While it is fathomable that the power of search and seizure of digital evidence requires no warrant that is to improve the effectiveness during an investigation, it is susceptible to the possibility of abuse which results in unfairness.

More complex digital evidence analysis and acquisition have been involved in the digital investigation system. Nowadays, the processing and storage of digital data might be involved in cloud computing. The survey conducted in Wales evaluated that, across four sectors 8% of the industries experienced at least one crime at a time in 12 months, before the survey was conducted. Many countries have endorsed cyber laws and acts for their states after observing the threats which are brought by the result of information and technological progressions striking the whole planet [34]. They ensured that there is a survival of protection and control for customers from being victims to the cyber-related crimes that are always posturing safety risk through cyber media.

Due to the commencement of information and technological development in the country, Malaysia is not excused from the performance of associated cyber acts. This is to make sure that there are some rules of harmony or law among the public, particularly to undertake cybercrime. The acts included the Computer Crime Act 1997, Communication and Multimedia Act 1998, and Consumer Protection (Electronic Trade Transactions) Regulations 2012. All these statutes are carried out for improvements with communication and technological developments [35]. It assists in tackling the increasing abuse and misconduct particularly affecting computer securities. Rules and acts are appropriate with the change of era and time, with the introduction of new cybercrimes [36].

As such, it is a hard question to answer on the issues of adequacy and effectiveness in the practices or guidelines on search and seizure of digital evidence in Malaysia. This is because the performances or guidelines on the search and seizure of digital evidence in Malaysia are kept as confidential government documents and are unavailable to the public. Even though there is section 68 of the Communication and Multimedia Media Act 1998, however, it only provides for the power of the Commission to investigate any cases on the administration of the Communication and Multimedia Media Act 1998 Act only. Other provisions in this 1998 Act further specify the power to search and seize under Chapter 3 [12]. In other words, the Commission has control over the Internet users in Malaysia, has only the power to investigate offences under the Communication and Multimedia Media Act 1998 only. Similarly, different enforcement agencies would have the power to investigate offenses under their legislation. This piecemeal approach makes search and seizure of digital evidence in Malaysia ineffective due to limited experts and expertise as well as resources.

Besides that, the gathering of digital evidence is a complicated and tedious job and requires the hands of experts. The Association of Chief Police Officers of England Wales and Northern Ireland (ACPO) has provided guidelines on the handling and the search and seizure of digital evidence. The guideline by ACPO is known as the Good Practice Guide for Computer-Based Electronic Evidence (hereinafter referred to as the "ACPO Guidelines"). Whilst the ACPO Guidelines have no legal impact, their principles aim to be compatible with the nature of digital evidence, at the same time as being fair and effective as to respect the privacy of any individual involved in the procedure. The ACPO Guidelines provide the best possible steps to be taken during search and seizure during a criminal investigation. At crime scenes, they provide guidance on how to deal with common scenarios encountered during the investigation. The ACPO Guidelines, although not a legal instrument, are published to help the enforcement officers to follow good steps during the search and seizure procedure of digital evidence which ultimately tries to satisfy the legal requirement of admissibility of the seized digital evidence and not to breach the privacy of any individual. As such, the move by ACPO in the UK in publishing the ACPO Guidelines should be emulated in Malaysia to make the search and seizure of digital evidence fair and more effective.

6 Conclusion

Cybercrime and traditional crimes facilitated by the internet are a universal criminal phenomenon, which hazes the conventional distinction between threats to internal and external security i.e. criminality, military, and terrorist activity. The accountability of the online networks to operate for a variety of diverse ends, and the ability with which people may shift from one type of unlawful activity to another, suggested that territorialism hinders efforts to fight effectively with the misuse of technology. Presently, the national authorities in Malaysia have been overcoming jurisdictional constraints by organizing with the agencies who have the capability to respond better and understand the Internet-facilitated crimes [36]. Malaysia has a variety of laws that secure responsive information, which includes banking privacy laws, and laws that protect other confidential reports.

The World Council for Justice and law firms encourage the harmonization and evaluation of legal systems throughout the globe. The consideration of this idea on many great and many small steps are on the way to fulfill this idea. The reflection of this vision on the establishment of an International Court for Cyber Crime (ICCC) has been intended as the start of an international program to mark a significant milestone on a long road. Technology itself is the best weapon against online crime.

The increasing toll of cybercrime and criminal activities needs more attention and concentration from the global population. Many other steps have been taken in Malaysia by implementing various enforcement tools and effective technological tools that reduce the criminal activities that are ICT-facilitated. It has been observed that cybercrime is a worldwide principle of public policy in Malaysia that has goals of preventing and fighting with this structure of planned crimes, through elevating literacy rate and global awareness. With the cooperation of police forces and international enforcement agencies in Malaysia, many legislative efforts on regional, traditional, and global levels have been established. The law on search and seizure of digital evidence in Malaysia and its admissibility may be fair overall, but it is not as effective, revised, and comprehensive as compared to laws in England and Wales.

Malaysia has always been focused on preserving the territory and property of others in the virtual world. Malaysia should produce more computer forensic experts in digital evidence, within the police force and other enforcement agencies. However, cybercrime in Malaysia cannot only remain a province of law enforcement. The IT professionals and law enforcement agencies are needed to work hand in hand, and more attentively with the community to develop cyber-fighting bands that have the talent, authority, and the means to reduce the crimes of the internet more swiftly. In order to deal with the intricacy of digital evidence, the law on search and seizure must be well-matched with the complexity of the evidence. In this view, the laws of Malaysia must be inclusive and the guidelines must be available to the public as the laws in England and Wales. The individuals who handle the digital evidence from the time it is seized until its presentation in court must be competent. The judges must also appreciate the complexity and technicality of digital evidence.

7 Acknowledgements

We gratefully thank the School of Law, and Research & Innovation Management Centre, Universiti Utara Malaysia for the encouragement and support to complete this article.

References

1. Prasad, J. Ibrahim, R. and Abdul Manaf, F. Understanding Cybercrime in Malaysia: An Overview. Sains Humanika. 2014. 2(2), 109-115.
2. Leacock, C. Search and seizure of digital evidence in criminal proceedings. Digital Evidence & Elec. Signature L. Rev. 2008. 5. 221-232.
3. Gantz, J.F., Christopher C. Manfrediz, A. Stephen Minton, David Reinsel, Wolfgang Schlichting, and Anna Toncheva. The diverse and exploding digital universe: an updated forecast of worldwide information growth through 2011. 2008. An IDC White Paper.
4. O'Brien, C.. Global data set for explosion as 'internet of things' takes off. April 9, 2014. The Irish Times.
5. Fenu, G. and Solinas, F. Computer forensics between the Italian legislation and pragmatic questions. International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2013. 2(1), 9-24.
6. Dykstra, J. and Sherman, A.T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation. 2012. 9. S90-S98.
7. Levi, M. Regulating Fraud (Routledge Revivals): White-Collar Crime and the Criminal Process. 2013. London: Routledge.
8. Toma, S. V., Alexa, I.V, and Nistor, C. Methods of risk modeling in economic activities. Business Administration. 2022. 10(1), 38-42.
9. Petar, C., Cisar, S.M. and Bosnjak, S. Cybercrime and Digital Forensics – Technologies and Approaches. In DAAAM International Scientific Book. 2014. edited by B. Katalinic, 525-542. Vienna: DAAAM International. DOI:10.2507/daaam.scibook.2014.42
10. Termimi, M.A.A, Rosele, M.I, Meerangani, K.A, Marinsah S.A and Ramli, M.A. Women's Involvement in Cybercrime: A Preliminary Study. Journal of Advances in Humanities. 2015. 3(3), (2015): 266-270.

11. Roderic, B., Grabosky, P., Mamoun A., Bouhours, B. and Chon, S. An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology. 2014. 8(1), 1-20.
12. Ayub, Z. A., and M. Yusoff, H. Right of online informational privacy of children in Malaysia: A statutory perspective. UUM Journal of Legal Studies. 2018. 9(1), 221-241.
13. Malaysian Communications and Multimedia Commission. Internet User Survey 2020. 2020. Cyberjaya, Malaysia: MCMC.
14. Aminnezhad, A. and Dehghantanha. A. A survey on privacy issues in digital forensics. International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2014. 3(4), 183-199.
15. Mohamed, D. Investigating cybercrimes under the Malaysian cyberlaws and the criminal procedure code: Issues and challenges. Malayan Law Journal. 2012. 6.
16. Crime Survey for England and Wales (CSEW), Office for National Statistics. Dataset Crime in England and Wales: Additional tables on fraud and cybercrime year ending December 2018. April 25, 2019. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables.
17. Office for National Statistics. Overview of fraud and computer misuse statistics for England and Wales. January 25, 2018. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25#which-groups-in-society-are-most-likely-to-be-victims-of-fraud-and-computer-misuse
18. McGuire, M., and Dowling, S. Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75. 2013. Home Office, United Kingdom.
19. Office for National Statistics. Internet access – households and individuals, Great Britain: 2020. August 7, 2020. https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2020#internet-access-households-and-individuals-data
20. Holt, T. J. Examining the forces shaping cybercrime markets online. Social Science Computer Review. 2013. 31(2). 165-177.
21. Lusthaus, J. How organised is organised cybercrime?. Global Crime. 2013. 14(1), 52-60.
22. Losavio, M., Pastukov, and Polyakova, P. Cyber black box/event data recorder: legal and ethical perspectives and challenges with digital forensics. Journal of Digital Forensics, Security and Law. 2015. 10(4), 43-58
23. Martin, G. Fraud and recessions: Views from fraudsters and fraud managers. International Journal of Law, Crime and Justice. 2011. 39(3), 204-214.
24. Gasser, U, Zittrain, J.L., Faris, R and Jones, R.H. Internet monitor 2014: Reflections on the digital world: Platforms, policy, privacy, and public discourse. Berkman Center Research Publication. 2014.
25. Hamsi, A.S., Saiful Bahry, F.R., Mohd Tobi, S.N. and Masrom, M. Cybercrime over internet love scams in Malaysia: a discussion on the theoretical perspectives, Connecting Factors and Keys to the Problem. Journal of Management Research. 2015. 7(2), 169-181.
26. Aris, N.A, Mohd Arif, S.M., Othman, R and Mohamed Zain, M. Fraudulent financial statement detection using statistical techniques: The case of small medium automotive enterprise. Journal of Applied Business Research (JABR). 2015. 31(4), 1469-1478.
27. Jewkes, Y. and Yar, M. eds. Handbook of Internet crime. 2013. London: Routledge.
28. Taylor, M., Haggerty, J., Gresty, G and Hegarty, R. Digital evidence in cloud computing systems. Computer law & security review. 2010 26(3), 304-308.
29. Argy, P. N., and Mason, S. Electronic evidence: disclosure, discovery and admissibility. 2007. London: LexisNexis Butterworths.

30. Ayub, Z. A., and M. Yusoff, Z. Search and seizure of digital evidence and privacy issues in Malaysia. 2015. LexisNexis (A) 1, lviii.
31. Sonny, Z. The state of e-government security in Malaysia: Reassessing the legal and regulatory framework on the threat of information theft. 2012.(1st Taibah University International Conference on Computing and Information Technology, Madinah, Saudi Arabia. http://irep.iium.edu.my/27226/1/E-government_%26_Info_Security_print_for_proceedings.pdf
32. Hassan, K. H., Abdelhameed, A. and Ismail, N. Modern means of collecting evidence in criminal investigations: Implications on the privacy of accused persons in Malaysia. International Journal of Asian Social Science. 2018. 8(7), 332-345.
33. Kornblum, J. Preservation of Fragile Digital Evidence by First Responders. 2002. The Digital Forensic Research Conference DFRWS 2002 USA Syracuse, NY Aug 6th - 9th 2002. http://dfrws.org/2002/papers/Papers/Jesse_Kornblum.pdf
34. Sa'di, M.M., Kamarudin, A.R., Mohamed, D. and Ramlee, R. Authentication of electronic evidence in cybercrime cases based on Malaysian laws. Pertanika J. Soc. Sci. & Hum. 2015. 23(1), 153-167.
35. Ong, L. Awareness of information security risks: an investigation of people aspects (a study in Malaysia). 2015. Unpublished DBA thesis, Southern Cross University, Lismore, NSW.
36. Hu, Y.X.C., and Bose, I Cybercrime enforcement around the globe. Journal of Information Privacy and Security. 2013. 9(3), 34-52.