PAPER:

DIGITAL FORENSICS IN MALAYSIA

By **Aswami Fadillah Mohd Ariffin** and **Izwan Iskandar Ishak**

Introduction

The term digital forensics is still relatively new to Malaysia, even though our digital forensic analysts have appeared as an expert witness in several high profile cases. More awareness and promotion programmes have to be devised in order to educate the public, and in particular those in the legal communities.

Overall, digital forensics are one tool in helping to solve crimes, especially when crimes involves the use of computers or any digital devices such as mobile telephones or PDAs (it can be computer crime or computer related crime). Data stored in such devices may be recovered and presented as evidence in court. The accused may, for example, try to delete any data stored in their computer with the intention of destroying evidence and avoiding successful prosecution. However, with digital forensic technology, any data that has been deleted may still be recovered. This certainly will help the court in adjudicating the case presented.

Digital forensics evidence: the legal framework

As a general rule, evidence is admissible if it is lawfully admitted at trial. At the time of writing this paper, the Malaysian Evidence Act 1950 only deals with the admissibility of documents produced by computers and of the statement contained in the document.[1] A new provision, S90A is an exception to the hearsay rule, and provides that a document produced by a computer or a statement contain therein shall be admissible as evidence of any fact stated in the document whether or not the person tendering the same is the maker of such document or statement.[2]

Section 90A of the Malaysian Evidence Act 1950 provides as follows:-

> 90A. Admissibility of documents produced by computers and of statements, contained therein.
> (1) In any criminal or civil proceeding a document produced by a computer or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.
> (2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.
> (3) (a) It shall be sufficient, in a certificate given under subsection (2), for a matter to be stated to the best of the knowledge and belief of the person stating it.
> (b) A certificate given under subsection (2) shall be admissible in evidence as prima facie proof of all matters stated in it without proof of signature of the person who gave the certificate.
> (4) Where a certificate is given under subsection (2), it shall be presumed that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the period during which the document was produced.
> (5) A document shall be deemed to have been produced by a computer whether it was produced by it directly or by means of any appropriate equipment, and whether or not there was any direct or indirect human intervention.
> (6) A document produced by a computer, or a statement contained in such document, shall be admissible in evidence whether or not it was produced by the computer after the commencement of the criminal or civil proceeding

[1] *Section 90A of the Malaysian Evidence Act 1950 (Act 56), introduced by the Evidence (Amendment) Act 1993.*

[2] *Augustine Paul, Evidence Practice and Procedure, (2nd edn, Malayan Law Journal, Kuala Lumpur, 2000), 639.*

or after the commencement of any investigation or inquiry, in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

(7) Notwithstanding anything contained in this section, a document produced by a computer, or a statement contained in such document, shall not be admissible in evidence in any criminal proceeding, where it is given in evidence by or on behalf of the person who is charged with an offence in such proceeding the person so charged with the offence being a person who was-

(a) responsible for the management of the operation of that computer or for the conduct of the activities for which that computer was used; or

(b) in any manner or to any extent involved, directly or indirectly, in the production of the document by the computer.

Opinion of experts in Malaysia

The difference between an expert and a lay witnesses is that the former gives opinion evidence and the latter gives factual evidence. The opinion of an expert is based on the facts in a case, and the facts must be proved by admissible evidence.[3]

The status of digital forensic evidence is not clearly mentioned in the Malaysian Evidence Act 1950. However, the admission of specialist evidence may be comfortably admitted in relation to the issue of admissibility of expert evidence under the Act. This is on the ground that the courts need a digital evidence specialist to testify on the digital forensic evidence tendered in a criminal proceeding. Acceptance of expert opinion is regulated by Section 45 of the Malaysian Evidence Act 1950 which provides as follows:-

45. Opinions of experts

(1) When the court has to form an opinion upon a point of foreign law or of science or art, or as to identity or genuineness of handwriting or finger impressions, the opinions upon that point of persons specially skilled in that foreign law, science or art, or in questions as to identity or genuineness of handwriting or finger impressions, are relevant facts.

(2) Such persons are called experts.

From the wording of the Act, it is suggested that a digital evidence specialist may come under the term 'science or art'. In the case of *Chou Kooi Pang & Anor v Public Prosecutor*,[4] Yong Pung How CJ expressed the view that expert opinion is only admissible to furnish the court with scientific information which is likely to be outside the experience and knowledge of a judge. The purpose of expert testimony is for the court to have the benefit of the acquired knowledge of the expert.[5] An expert must be skilled in his field and this does not necessarily mean that he has made a special study of his subject, but it can also be obtained from experience.[6]

Clearly the test that should be administered to determine whether a person is an expert or not is highly relevant. Muhammad Azmi SCJ in *Junaidi Abdullah v Public Prosecutor* indicated that:-

> 'The speciality of the skill required of an expert witness under s. 45 would depend on the scientific nature and complexity of the evidence sought to be proved. The more scientific and complex the subject matter, the more extensive and deeper will the Court be required to enquire in the ascertainment of his qualification or experience in the particular field of art, trade or profession.'[7]

In Malaysia, the procedure for the admittance of expert evidence is governed by section 399 of the Criminal Procedure Code.[8] Section 399(1) of the code provides:-

399. Reports of certain persons.

(1) Any document purporting to be a report under the hand of any of the persons mentioned in subsection (2) upon any person, matter or thing examined or analysed by him or any document purporting to be a report under the hand of the Registrar of Criminals upon any matter or thing relating to finger impressions submitted to him for report may be given in evidence in any inquiry, trial or other proceeding under this Code unless that person or Registrar shall be required to attend as a witness-

(a) by the Court; or

(b) by the accused, in which case the accused shall give notice to the Public Prosecutor not less than

[3] *Hodge M. Malek, general editor, Phipson on Evidence (16th edn, Sweet & Maxwell, 2005) 33.09-33.10.*

[4] *[1998] 3 SLR 593 at 598.*

[5] *Jeremy Gans and Andrew Palmer, Australian principles of evidence, (2nd edn, Sydney, Cavendish Publishing, 2004), at 246.*

[6] *Per Suffian LP in Public Prosecutor v Mohamed bin Suleiman, [1982] 2 MLJ 320 at 322.*

[7] *[1993] 4 CLJ 201.*

[8] *Harcharan Singh Tara, Expert Evidence in Civil and Criminal Cases, [1995] 2 MLJA 45.*

three clear days before the commencement of the trial:

Provided always that in any case in which the Public Prosecutor intends to give in evidence any such report he shall deliver a copy of it to the accused not less than ten clear days before the commencement of the trial.

Section 399(2) of the Code, provides that 'persons' include officers of the Institute for Medical Research, government medical officers, chemists in the employment of any government in Malaysia or of the government of Singapore, any person appointed by the Minister by notification in the Gazette, to be a Document Examiner, Inspector of Weights and Measures appointed as such under any written law relating to weights and measures in force in Malaysia, and any person or class of persons to whom the Minister by notification in the Gazette declares that the provisions of this section shall apply.[9] As a result, it is clear that a digital evidence specialist is not included as 'person' under the Code at present. Digital forensic evidence remains new, and has yet to be embraced by the legal systems in the country.

Cybersecurity Malaysia: its role in digital forensics

Recognizing the need for the development of computer forensic expertise in the country, the government under the Ministry of Science, Technology and Innovation has set up an agency under its control to deal with computer forensic matters. The agency is known as CyberSecurity Malaysia (CSM). This agency is established to prepare Malaysia in facing the challenges in computer forensic evidence.

In the age of information technology, computers are used everywhere. Demand for digital forensic services has shown a tremendous growth over the past few years. Criminals use computers to facilitate their criminal intentions. Their activities, plans, or even information related to their crime may be stored in a computer. In a criminal proceeding, it is necessary to prove that the computer is associated with the accused. This is when an expert is needed to set his expertise in the area and provide an explanation to the court. CyberSecurity Malaysia has been the focal point in the country to assist in providing these services. This can be inferred from the statistics of cases referred to the agency for the past few years. The figure shows the trust and confidence of the public and private sectors towards the expertise of CyberSecurity Malaysia in the area of digital forensics.

The following diagram shows the overall statistics that received between 2002 and 2008. The cases are divided into two categories of forensics analysis and data recovery. The requests for forensic analysis normally comes from the local law enforcement agencies and regulatory bodies such as the Royal Malaysian Police, National Bank of Malaysia and such like. It is the job of CSM to provide a scientific analysis of digital evidence in order to inculpate or exculpate the person under suspicion. In 2008, the number of cases analysed is anticipated to be greater than 2007.

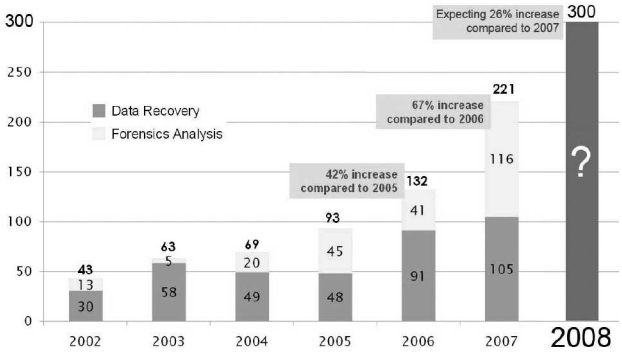

Figure 1 **Cases received by CSM between 2002-2008**

CyberSecurity Malaysia provides digital forensics services to the country. These services include: the secure collection and imaging of digital evidence; digital evidence investigation, analysis and presentation; analysis of audio and video evidence (analogue evidence); digital evidence protection and data recovery.

In digital evidence investigations, CyberSecurity Malaysia has worked closely with the law enforcement agencies in the country. The scope of collaborations include: joining law enforcement team in searches to identify digital devices that may contain relevant digital evidence; identifying digital evidence through the process of imaging to separate hard disk to preserve the integrity of the original evidence; performing analysis on the imaged copy of the evidence; documenting all findings in a report as required by the authorities, and presenting the final findings to the law enforcement body and the court.

[9] *See section 399(2) of the Malaysian Criminal Procedure Code.*

Digital evidence requires special handling skills and attention, and just by having the technology and the appropriate tools will not guarantee the success of a computer forensic exercise.

Expert witness: the completion of the perfect cycle

Analyzing evidence contained in a computer requires special skills. Equipped with specific knowledge together with precise tools, most evidence stored in a computer may be retrieved. The evidence will then be presented in the court whenever necessary to support the case presented. In presenting the evidence, it is quintessential to call an expert witness, or to have his report to elucidate the evidence. This is where CyberSecurity Malaysia expertise may be required, to assist the parties and the judges in understanding the evidence tendered in criminal proceedings.

As criminals use more effective means of carring out their acticities, cases become more complex and difficult. Digital forensic services provided by CyberSecurity Malaysia were formally announced in 2002. Since then, the agency has worked closely with various parties, including law enforcement agencies, government agencies, financial institutions and the private sector. The law enforcement agencies include the Royal Malaysian Police, Royal Malaysian Customs, Ministry of Domestic Trade & Consumer Affairs, Securities Commissions, Central Bank of Malaysia and the Malaysian Communications & Multimedia Commission.

A positive development in the legal system of the country occurred when the expertise of CyberSecurity Malaysia was recognized in the case of *PP v Teoh Kee Hean*,[10] in respect of an action under the Copyright Act 1987 which was tried on 7 and 8 March 2007, the court called upon two of the officers who performed the digital forensic analysis at CMS on the evidence to testify and provide expert opinions pertaining to the evidence in question.

In the case of *PP v Ching Cheng Kiong*,[11] a case relating to credit card fraud activity. The digital evidence was in the format of video from CCTV. Digital evidence specialists conducted video forensics analysis and produced a report on the findings. The analyst then appeared in court to testify on the digital evidence based on the analysis.

Subsequently, CyberSecurity Malaysia analysts were called to appear as expert witness in number of high profile cases, such as the Altantuya Sharibu murder trial[12] between 6 and 21 November 2007 and the VK Lingam[13] tape recording on 15 January 2008. The previous cases have created a significant effect on the importance of digital forensics. As such, it is expected that several other cases handled by CyberSecurity Malaysia will be called by the court in the future.

CyberSecurity Malaysia: the focal point in digital forensics

Digital evidence requires special handling skills and attention, and just by having the technology and the appropriate tools will not guarantee the success of a computer forensic exercise. It is very much dependant on the person who is responsible for performing the task required. Digital evidence specialists from CyberSecurity Malaysia are certified in their respective field and they are specialized.

For the purposes of presenting credentials in a court, certification is compulsory, and may include the ENCE (ENCASE Certified Examiner from Guidance Software), GCFA (GIAC Certified Forensic Analyst from SANS Institute), CEH (Certified Ethical Hacker from EC Council) and CWSP (Certified Wireless Security Professional from Planet 3 Wireless Inc). Other than professional certifications, some of the analysts are involved in digital forensic master and postgraduate (PhD) programs. This is vital and part of the research and design efforts in the digital forensics field.

Apart from having a certified personnel, systematic laboratory management is an equally important element for laboratory accreditation process.

[10] *Magistrate Court, Penang, Malaysia.*
[11] *Sessions Court, Penang, Malaysia.*
[12] *A local case involving one prominent political figure in the country.*
[13] *A local case involving a prominent lawyer and the Current Chief Justice on the appointment of Senior Judges in Malaysia; for more information, see the entry in the Wikepedia: http://en.wikipedia.org/wiki/Royal_Commission_of_Inquiry_into_the_Lingam_Video_Clip.*

CyberSecurity Malaysia digital forensics laboratory is in the process of obtaining accreditation from the American Society of Crime Laboratories Directors (ASCLD). ASCLD is a non profit professional society of crime laboratory directors and forensic science managers dedicated to promoting excellence in forensic science. It is the aim of CyberSecurity Malaysia to get such certification by 2010.

In the digital forensics laboratory, numerous tools are used to perform digital forensic services. Some of the tools are commercial and others are based on open source. However, we have acquired most of the tools that are widely used by most forensic laboratories around the world. These tools are EnCASE and FTK for acquisition and analysis, HELIX from open source, XRY and PARABEN for mobile forensics and recently VIDEO FOCUS for audio video forensics. Nevertheless, the emphasis is more on the technology and science knowledge rather than dependence on tools. Technology evolution is constant and research and design activities in CyberSecurity Malaysia are also constant. Apart from common computer forensics, generally, all the analysts are specialist in their respective area, such as audio and smartcard forensics.

The future

Although the legal framework might not be as comprehensive in comparison to other European countries, Malaysia has made tremendous developments in the area of digital forensics. With the establishment of CyberSecurity Malaysia, the country has a good platform to be the focal point for computer forensic in the region. The increased need for digital forensics may eventually change the legal framework, so that the interpretation and evaluation of computer forensic evidence may improve in the future.

Aswami Fadillah Mohd Ariffin is the Head of Digital Forensic, CyberSecurity Malaysia and Izwan Iskandar Ishak is a Senior Executive, Strategic Policy & Legal Research of CyberSecurity (Malaysia).