ARTICLE:

DIGITAL FORENSICS INSTITUTE IN MALAYSIA: THE WAY FORWARD

By **Aswami Ariffin, Jill Slay** and **Husin Jazri**

The number of internet users in Malaysia fell by 1.1 per cent in 2010. Simultaneously, cyber crimes and cyber related crimes handled and resolved by CyberSecurity Malaysia's Digital Forensics Department increased by 101.9 per cent. Despite this accomplishment, there are two notable concerns: the increase in reported crimes when the number of internet users dropped, and the operation of digital forensics laboratories and research activities are not coordinated. This paper considers the digital forensics landscape in Malaysia by analyzing the problems encountered, its achievements and a brief comparison with Japan. A Digital Forensics Institute is proposed as a way forward.

Introduction

In 2009, the number of internet users in Malaysia[1] was estimated by one market research organization as 16,902,600 from a population of 25,715,819. A year later, in 2010, the numbers estimated were 16,902,600 from a population of 26,160,256. To encourage its citizens to use the internet, the government is collaborating with TM Berhad,[2] a local broadband service provider, to improve the infrastructure and charge at a low price rate. Some states, for example Penang, provide free wireless connection.[3]

In the same period, cyber crimes and cyber related crimes increased by 101.9 per cent. To address this problem, the government established CyberSecurity Malaysia in 1998, formerly known as National ICT Security and Emergency Response Centre or NISER. CyberSecurity Malaysia is a reference centre for cyber security and digital forensics, introduced to help resolve cyber crimes. To date, the overall digital forensics initiatives in Malaysia are progressing satisfactorily because all cases have been resolved[4] and there are some research publications.[5]

However, the problems faced by Malaysia include poor research coordination and lack of cooperation among agencies. Universities predominantly initiate most of the research efforts, with occasional discussion at national level in an attempt to harmonize requirements, activities and resources. Whilst some of the legal agencies have their own laboratories, publically available information on their systems are limited because of confidentiality. The problems include imprudent management, the failure to be cost effective, some redundancy, and a decentralized approach to the problems. The authors argue that these approaches need to be changed in the interests of an effective digital forensics service to deal more effectively with cyber threats that are increasing and becoming more difficult to resolve.

This paper analyses cyber crimes and cyber related crimes encountered in Malaysia. The efforts to mitigate the problems are discussed, such as digital forensics research, operational procedures, including the achievements of CyberSecurity Malaysia's Digital Forensics Department from 2000 to 2010. A brief comparison is made with Japan to illustrate the Japanese success in dealing with this issue for the purpose of learning from the Japanese experience, and to suggest that Malaysia consider the foundation of a Digital Forensics Institute to provide for a more coordinated and rational approach to this issue.

1 *Internet World Stats and International Telecommunication Union, Malaysia Internet Usage Stats and Marketing Report, http://www.internetworldstats.com/asia/my.htm. Note, this web site that is apparently run by Miniwatts Market Research; http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=190.*

2 *'TM to announce UniFi pricing today', TheEdge, 5 March 2010, http://www.theedgemalaysia.com/business-news/162295-tm-to-announce-unifi-pricing-today.html; http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=36.*

3 *Andrea Filmer, 'Penang launches statewide free WiFi project', The Star, 18 September 2008, http://thestar.com.my/news/story.asp?file=/2008/9/18/nation/20080918201219&sec=nation; myconvergence.com.my/main/images/stories/.../MyCon06_29.pdf.*

4 *CyberSecurity Malaysia, Digital Forensics – CyberCSI 2010 Annual Report, http://www.cybersecurity.my/en/services/digital_forensics/about/main/detail/1987/index.html.*

5 *Sundresan Perumal, 'Digital Forensic Model Based On Malaysian Investigation Process', International Journal of Computer Science and Network Security, volume 9 number 8 (August 2009), 38-44.*

Figures for cyber crimes

The Digital Forensics Department maintains statistics on cyber crimes, although not all cases are cyber crimes, but include an element of digital evidence in some form. An example is where a person is murdered, and the case requires the analysis of closed circuit television, or a mobile telephone and a digital video recorder features as part of the evidence. The crime will normally be termed as a cyber related case if it includes evidence from digital devices.

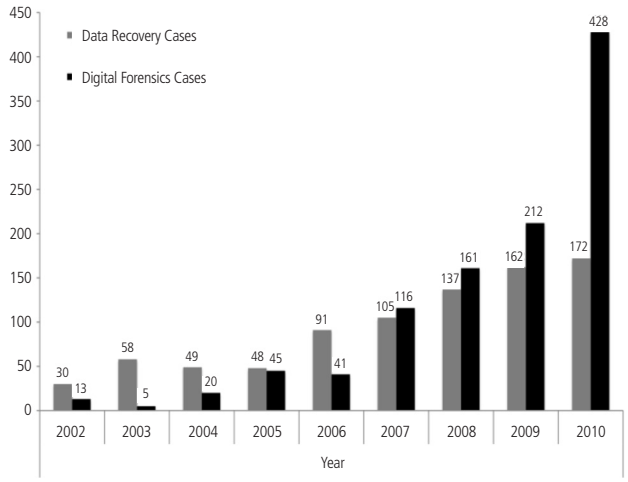

Figure 1. **Digital Forensics Department Case Statistics from 2002-2010**

From 2002 to 2010, the Digital Forensics Department managed 1,893 cases (Figure 1), including crime scene investigations with broad technical background. The cases included computer forensics, mobile telephone forensics, audio forensics, video forensics and data recovery.[6] A total of 600 cases from various legal agencies were analysed in 2010. Among the legal agencies that made referrals to the Digital Forensics Department were the Royal Malaysia Police, Royal Malaysian Customs Department, Malaysian Communications and Multimedia Commission, Companies Commission of Malaysia, Securities Commission Malaysia, Malaysian Anti-Corruption Commission, Ministry of Defense and Ministry of Domestic Trade, Cooperative and Consumerism. The Royal Malaysia Police was the highest contributor, with 246 cases.

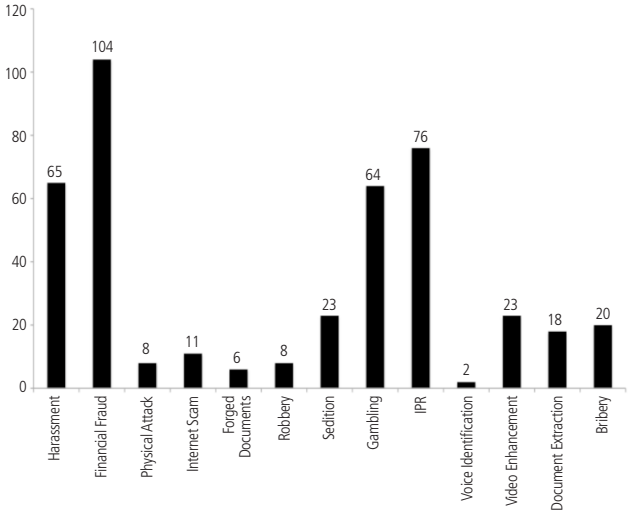

Figure 2. **2010 cases by category**

Cases of financial fraud (Figure 2) were the highest in 2010, involving pyramid and investment schemes. Second, with 76 cases, were illegal businesses and piracy of games, grouped under 'IPR'. Harassment cases were divided into three types: threats, blackmail and sexual. Document falsification (forgery of documents) such as forged passports and visas amounted to 6 cases. Internet scams, sedition, physical attacks, gambling, robbery, voice identification, video enhancement, document extraction and bribery recorded 11, 23, 8, 64 (higher than previous year due to the World Cup match), 8, 2, 23, 18, 20 cases respectively.

The Malaysia Computer Emergency Response Team (MyCERT[7]) is another department within CyberSecurity Malaysia that provides a public service called Cyber999 to assist and provide advice to Malaysian citizens on cyber related incidences. It handled 8,090 incidences in 2010, and the most frequent complaint was fraud, with 2,212 requests for assistance. Other complaints included intrusion, spam, cyber harassment, denial of service, reports on vulnerabilities and matters related to the content of web sites.[8]

Examples of problems encountered in Malaysia

There are challenges in operating a digital forensics service because cases of cyber crime and the use of

6 *http://www.cybersecurity.my/en/services/digital_forensics/about/main/detail/1986/index.html.*
7 *http://www.mycert.org.my.*
8 *For MyCERT Incident Statistics figures, see http://www.mycert.org.my/en/services/statistic/mycert/2012/main/detail/836/index.html.*

digital devices linked to crimes have increased every year. The diversity of the technologies used has been the main problem for the Digital Forensics Department, and still is. For instance, some of the cases reported in 2010 included hard disks that were in a poor condition and malfunctioned. Forensic data recovery of the hard disk requires specialized techniques, tools and clean facilities.[9]

Forensic data recovery of a digital video recorder is an example, and expertise in this subject is urgently needed because cases in which video evidence has been found are increasing by approximately 15 per cent annually. The need for such expertise is further justified at a time when the government is installing more close circuit televisions.[10]

If forensic data recovery of a digital video recorder fails, other forensic analyses such video authentication, image enhancement and identification could not be conducted. The major problems faced by the digital forensics specialists are usually because they are asked to forensically examine customized, proprietary and corrupted digital video recorders with a variety of video file formats. This makes video files with timestamp extraction and playback more complicated. Using commercial and open source digital forensics tools are often ineffective because they are not able to analyze digital video recorders.

Digital forensics research in Malaysia

It is suggested that innovation[11] and investment is the answer to the problem faced by the authorities in Malaysia. The Digital Forensics Department has a research unit to handle operational matters. Hypothetically, analyzing data streams can resolve the forensic data recovery of digital video recorder complexity. Information on the forensic data recovery of digital video recorder techniques and tools are not freely available because of manufacturing secrecy. Existing research on this topic is limited, and empirical examination is currently being carried out by the Digital Forensics Department. The aim is to produce best practice guidelines, and a software tool will be developed to assist digital forensics specialists in their work. Nevertheless, a scientifically proven framework with three main steps is completed and is referred to in Figure 3.

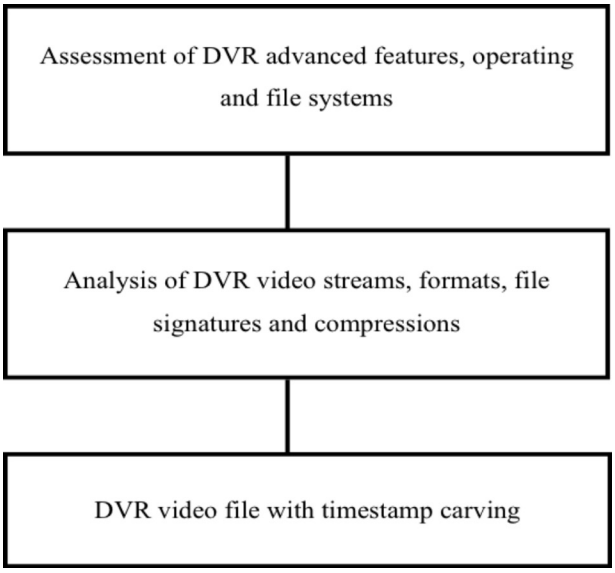

Figure 3. **Framework of Forensic Data Recovery of Digital Video Recorder**

Digital forensics procedures in Malaysia

The Digital Forensics Department[12] is frequently referred to if the crime needs a thorough digital evidence analysis involves criminal proceeding with the aim of bringing the offender to justice. The service request is made by the respective legal agency by handing over the evidence, and a case file will be opened to collect all the details. The two parties will maintain constant communications, and an expert witness will maintain records on the progress of the technical analysis until the handover of the final report and possible appearance in court. All investigations and criminal proceeding for legal proceedings are handled by the respective law legal agencies.

In principle, the standard operating procedures of the Digital Forensics Department consists of identification, preservation, recovery, analysis and presentation of digital evidence. This follows the ASCLD/LAB-International requirement,[13] an American Society of Crime Laboratory Directors Laboratory Accreditation Board[14] and ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories. The aim is to provide for high quality and trustworthy

9 *Charles H. Sobey, Laslo Orto and Glenn Sakaguchi, 'Drive-Independent Data Recovery: The Current State-of-the-Art', The IEEE Transactions on Magnetics (2007), 1-6.*

10 *Nancy Nais, 'More CCTVs planned for Putrajaya', New Straits Times, 28 March 2012, http://www.nst.com.my/nation/general/more-cctvs-planned-for-putrajaya-1.67398.*

11 *Kara Nance, Brian Hay and Matt Bishop, 'Digital Forensics: Defining a Research Agenda', in Proceedings of the 42nd Hawaii International Conference on System Sciences (2009).*

12 *http://www.cybersecurity.my/en/services/digital_forensics/about/main/detail/14/index.html?mytabsmenu=1*

13 *http://ascld-lab.net/Applications.html.*

14 *http://ascld.org/.*

foundations for the work undertaken by the Digital Forensics Department.[15] The agencies that refer work to the Digital Forensics Department value such accreditation, and consequently they send more work to be processed by the Digital Forensics Department, even if some of them have their own digital forensic laboratories.[16]

All digital forensic specialists must adhere to the standard operating procedures strictly, from the moment the evidence is accepted or obtained during the crime scene investigation, until the analysis is completed. This is to avoid any challenges in court relating to the procedures adopted by the digital evidence specialist.

Additionally, a set of digital video recorder data recovery best practice guidelines are going to be developed by the Digital Forensics Department, and will be recommended for reference when giving opinion evidence. This kind of document is scientifically produced and difficult to rebut by the opposing party.

The standard operating procedures of the Digital Forensics Department also include guidelines in giving expert witness testimony. They are: to understand the act used to charge the suspect and other related information during the criminal proceedings; to review, validate and finalize their report findings; statements taken from the expert witness for court submission and their legal standing; to understand the prosecution course of action; the appropriate expert witness presentation style; to understand how cross examination is being conducted, and overall post-event analysis.

The opinion of an expert witness is based on the facts in a case and must be proven by admissible evidence. This is on the ground that the courts need a digital evidence specialist to testify on the digital forensics evidence tendered in a criminal proceeding. Acceptance of expert opinion is regulated by Section 45 of the Evidence Act 1950 which provides:

> 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.

In Malaysia, the procedure for admittance of expert evidence can be noted from section 399 of the Criminal Procedure Code Act 593. A digital forensics specialist report produced by CyberSecurity Malaysia is recognized under section 399(2)(f) of the Criminal Procedure Code, which reads as follows:

> Reports of certain persons
>
> 399. (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 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.
>
> (2) The following are persons to whom the provisions of this section apply:
>
> (a) officers of the Institute for Medical Research;
>
> (b) Government Medical Officers;
>
> (c) chemists in the employment of any Government in Malaysia or of the Government of Singapore;
>
> (d) any person appointed by the Minister by

15 *Jill Slay, Yi-Chi Lin, Benjamin Turnbull, Jason Beckett and Paul Lin, ' Towards a Formalization of Digital Forensics' , in Gilbert Peterson and Sujeet Shenoi, eds, Advances in Digital Forensics V (2009, Springer, Boston), 37-47.*

16 *http://www.sprm.gov.my/.*

notification in the Gazette, to be a Document Examiner;

(e) Inspector of Weights and Measures appointed as such under any written law relating to weights and measures in force in Malaysia; and

(f) any person or class of persons to whom the Minister by notification in the *Gazette* declares that the provisions of this section shall apply.

(3) The persons referred to in subsection (2) and the Registrar of Criminals are by this Code bound to state the truth in reports made under their hands.

Digital forensics has been used in Malaysia's courts to inculpate or exculpate a suspect.[17] Courts accept digital evidence, and digital forensic experts are called to provide expert opinion. In 2009, eleven cases were taken to court under sections 211 and 233 of the Malaysian Communications and Multimedia Act 1998.[18] The suspects were charged for posting coarse comments on web sites, short message service (SMS) and e-mails that insulted the Sultan of Perak (one of the states in Malaysia).[19]

Digital forensics achievements in Malaysia

The Malaysia government supports the development of the Digital Forensics Department laboratory. This is important, because the cost is high. Equally important is to carefully plan for the quality of the people involved, as well as the quality of the process and facilities – all of which are capable of adding to its success.

The progress must be in parallel that includes training, laboratory accreditation and installation of equipment (plus future expansion). Figure 4 summarizes the achievements of the Digital Forensics Department between 2000-2010; and as of 2011, the Digital Forensics Department laboratory is ASCLD/LAB accredited.

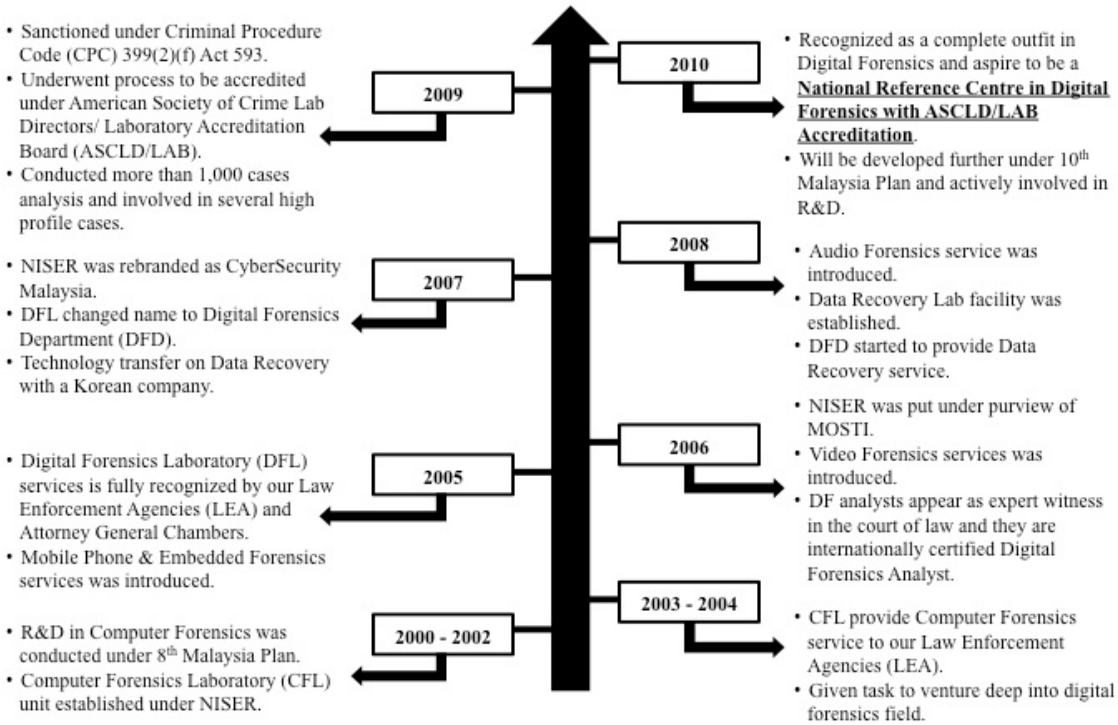

Figure 4. **The Digital Forensics Department Achievements from 2000 to 2010**

17 *Aswami Fadillah Mohd Ariffin and Izwan Iskandar Ishak, 'Digital Forensics in Malaysia', Digital Evidence and Electronic Signature Law Review 5 (2008), 161-165.*

18 *http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=30*

19 *Jacqueline Ann Surin, '11 cases brought to court under CMA', The Nutgraph, 21 October 2009, http://www.thenutgraph.com/eleven-cases-brought-to-court-under-cma/.*

A brief comparison with Japan, discussion and future work

In 2010, internet users in Japan[20] were listed by one marketing organization as being 99,143,700 from a population of 126,804,433 with a penetration rate of 78.2 per cent. The annual growth difference between Japan and Malaysia was only 13.6 per cent. Taking into account that Japan is a developed country with a better infrastructure, the gap is small, which illustrates the government of Malaysia's objective to increase the number of people that used the internet in Malaysia is deemed to have been fruitful.

In relation to cyber crime, the reported cases in Japan have increased since 2003.[21] Fraud and fraud using the internet were the highest in 2007 with 1,512 and 1,229 cases respectively. The lowest was cyber crime relating to copyright, with 165 cases. Cases of fraud were common, and it is alarming to note that it is increasing in Japan and Malaysia.

The number of users of the internet in Japan is higher than in Malaysia, which means it is expected that their cyber crime cases were also higher. In Malaysia, even if we combine the reported cases from the Digital Forensics Department (221 cases) and MyCERT (1,038 incidences), the Malaysian figures are lower than the number of cases in Japan (4,082 cases) in 2007. Even though the number of cases in Japan was higher, it is considered a better figure in proportion, because the number of internet users in Japan was about six times higher than in Malaysia. In this regard, Malaysia must take preventative measures to try and reduce the number of reported cases, rather than resolving them.

Unfortunately, the digital forensics agencies in Malaysia operate in such a way as not to communicate with each other. Perhaps this attitude is because of the confidential nature of the work conducted. There are no examples of any effort to share experience, either generally, or to share expertise. In conducting research for this paper, the authors failed to find evidence of an formal meeting between the agencies, with the exception of the 'Digital Forensics Forum For Researchers and Academicians' and 'Digital Forensics Closed Session Seminar For Law Enforcement Agencies, Regulatory Bodies and Deputy Public Prosecutors' organized by CyberSecurity Malaysia's Digital Forensics Department in 2010, the of which aim was to bridge the gap between practitioners and researchers.[22]

This area deals with fast evolving technologies, and the latest threats require the development of new plans in order for the forensics services to stay relevant. The Digital Forensics Department statistics demonstrate that the cases will get more difficult, and cloud forensics is just one practical example of the changes that are occurring. Operational cooperation is needed due to the borderless nature of crime, and it should be extended to research as well. This new approach will be in a better position to resolve challenging cases.

In Japan, one notable sign of progress is the setting up of 'The Institute of Digital Forensics'.[23] This is a non-profit organization whose brief is to look into the area of technology development, globalization, legal reform, public awareness, civilian research and development and higher education. It acts as the intermediary between the government, the national police agency, industry, education and promoting the development of digital forensics in Japan.

It would be good to have a similar institute in Malaysia. This noble idea is to maintain the progress of digital forensics. It is justifiable by considering the contribution of the Digital Forensics Department since 2000. With the formation of such an institute, more programs can be considered. For future work, it is recommended that the programs noted below should be considered as a matter of urgency.

No	Program	Objective
1.	Research and Development	Conduct research based on operational or anticipated problems. Outputs are turned into innovative process (technique) and product (tool). Less dependence (independent) on commercial tools. Capable of resolving own problems by sharing case complexity among practitioners and researchers. Creation of research database. Coordinated activities. Optimization of funding.
2.	Globalization	Able to work with counter part. Ensure quality of service on par with others. Standardization of approach and solution. Counter act against globalize crime. International recognition.

20 *Internet World Stats and International Telecommunication Union, Japan Internet Usage Stats and Marketing Report, http://www.internetworldstats.com/asia/jp.htm.*

21 *Jigang Liu and Tetsutaro Uehara, 'Computer Forensics in Japan: A Preliminary Study', International Conference on Availability, Reliability and Security ARES 2009 (IEEE Computer Society, 2009), 1006-1011.*

22 *http://www.cybersecurity.my/en/events/2010/main/detail/1837/index.html.*

23 *http://www.digitalforensic.jp.*

3.	Legal Reform	Better protection for the digital forensics specialist. New act specifically for digital evidence. Mutual treaty.
4.	Public Awareness	Increasing public confidence. As a deterrence to crime. More economic activities will be conducted.
5.	Higher Education	Engaging with university researchers on the relevant topics. Providing inputs for degree programs. Provide better funding.
6.	Cooperation	Sharing of general case information among digital forensics laboratories. For national level engagement against cyber crime. Research and development initiatives can be included with the aim to reduce cost. Sharing of resources to avoid redundancy. Optimizing operation and development fund.
7.	Others	Better recognition for the digital forensics specialist. Centralized service with state of the art facilities. Control environment with secured system to protect evidence. Focus workforce by separating investigation and analysis tasking. Produce more researchers at PhD level.

Table 1. **New programs for Digital Forensics Institute in Malaysia**

Conclusion

Digital forensics in Malaysia is not new, and CyberSecurity Malaysia has been promoting the digital forensics service since 2000. In the span of ten years, the Digital Forensics Department has proved to be successful. From merely providing computer forensic service, it now provides mobile telephone forensics, audio forensics, video forensics and data recovery. As a result, cyber crime and cyber related crime cases have been resolved.

Without the support of the government of Malaysia by providing operational and development funds, the achievements would not have been realized. In order to stay relevant, Malaysia should not be complacent, because the threats will not diminish. In fact, it is safe to say that they will be more complicated in the near future. As a way forward, it timely to establish a Digital Forensics Institute in Malaysia. The aim should be to bring the service, capability and capacity to the next level.

Aswami Ariffin has a bachelor of engineering in electronics from the University of Liverpool and master in management from University of Malaya and works for CyberSecurity Malaysia, Malaysia. Currently, he is pursuing his PhD at the University of South Australia in digital forensics. In 2009, he was awarded 'Information Security Leadership Award' by ISC2 for digital forensics contribution in Malaysia.

aswamifadillah@gmail.com

Jill Slay is a professor and dean of research of Information Technology, Engineering and the Environment of University of South Australia.

jill.slay@unisa.edu.au

Professor Husin Jazri is a Director and the Chief Executive Officer of CyberSecurity Malaysia, Malaysia.

husin@cybersecurity.my