Digital Forensics Institute in Malaysia: The Way Forward

Digital forensics initiatives in Malaysia are progressing well. Proficiency as a practitioner is acknowledged since 2000 and for research there are numerous paper publications. However, it requires further endeavor to join the standing of others. This paper aims to study digital forensics landscape in Malaysia. Establishment of an institute is proposed as a way forward.

Introduction [Heading type A]

Malaysia Internet users[1] were estimated at 16,902,600 from a population of 26,160,256 in 2009. In Japan[2], 2010, their Internet users were 99,143,700 from a population of 126,804,433. Penetration rate was 64.6% for Malaysia and Japan was 78.2% with a difference of 13.6%.

Malaysia outcome was positive and expected to grow significantly. Collaboration between the government and TM Berhad[3] (local broadband service provider) to improve the connection is an indicator. A low price rate would continuously encourage its citizens to leverage the Internet for knowledge. Some states provide free wireless connection[4].

Nonetheless, cybercrimes have risen and they are inevitable. The government is not deterred and founded Malaysia Computer Emergency Response Team or MyCERT.[5] A public service called Cyber999 is launched to assist and provide advisory to Malaysian on cyber related incidences.

Digital forensics is another full-fledge service provided by CyberSecurity Malaysia. Digital Forensics Department or DFD is frequently referred if the incidence needs thorough digital evidence analysis, involves legal proceeding and bringing the offender to justice. The service request is made by the respective law enforcement agencies (LEA) and investigation or court administration task belongs to them.

---

[1] Internet World Stats and International Telecommunication Union, *Malaysia and Japan Internet Usage Stats and Marketing Report*, http://www.internetworldstats.com/asia/my.htm and http://www.internetworldstats.com/asia/jp.htm (May 2012).

[2] This paper includes brief comparison with Japan on cybercrime and digital forensics.

[3] Wikipedia, *UniFi*, http://en.wikipedia.org/wiki/UniFi#cite_note-0 (May 2012).

[4] http://thestar.com.my/news/story.asp?file=/2008/9/18/nation/20080918201219&sec=nation (September 2008).

[5] MyCERT, www.mycert.org.my (February 2012).

This paper analyzes cybercrimes, cyber related crimes and problems encountered in Malaysia. Mitigation efforts are discussed such as digital forensics research and procedures including progress. Comparison is made with Japan and to move forward, a Digital Forensics Institute in Malaysia (DFIM) is proposed.

Figures for cybercrimes [Heading type A]

MyCERT is under CyberSecurity Malaysia, a government owned agency specializes in cyber security and reporting to Ministry of Science Technology and Innovation (MOSTI). It handled 8,090 incidences (Figure 1) in 2010 and the top was fraud with 2,212. Others included intrusion, spam, intrusion attempt, cyber harassment, denial of service, vulnerabilities report and content related.

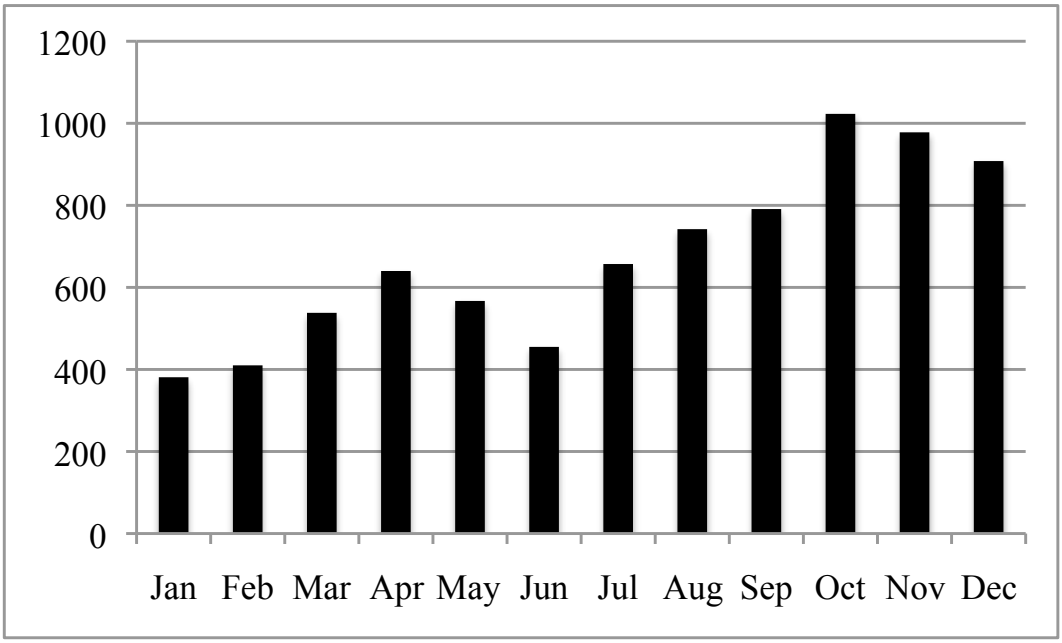

Figure 1. MyCERT Incident Statistics in 2010

DFD has its own case statistics and not all cases are cybercrime per se. One of the examples is homicide case that requires analysis of closed circuit television (CCTV) or mobile phone digital video recorder (DVR). This is normally termed as cyber related case.

From 2002 to 2010, DFD managed 1893 cases including onsite investigations with broad technical background. 600 cases (Figure 2) of various LEA were successfully analyzed in 2010. Among them were 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. Royal Malaysia Police was the highest contributor with 246 cases.

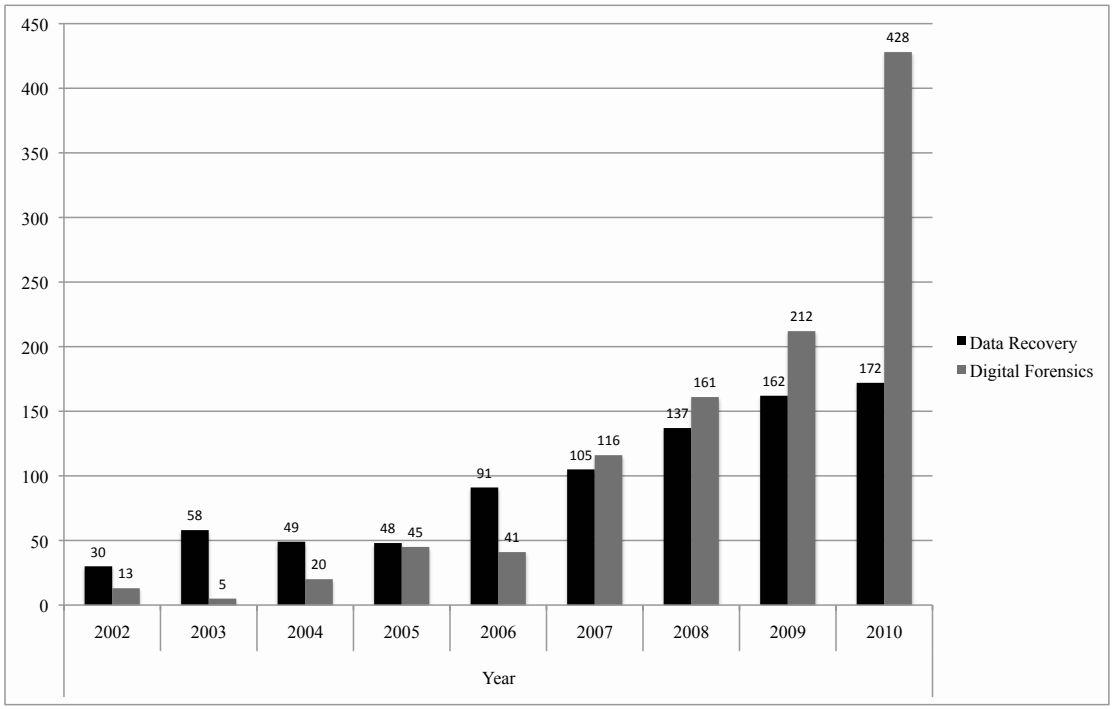

Figure 2. DFD Case Statistics from 2002-2010

Financial fraud case[6] (Figure 3) was the highest in 2010. Mainly, it involved pyramid and investment schemes. Illegal business and game piracy were grouped under 'Copyright & Others' and it was second with 76 cases.

Harassment case was divided into three types: threat, blackmail and sexual. Document falsification (forgery of documents) such as fake passport/visa was 6 cases. Internet scam, sedition, physical attack, gambling, robbery, voice identification, video enhancement, document extraction and bribery recorded 11, 23, 8, 64 (higher than previous year due to World Cup match), 8, 2, 23, 18, 20 cases respectively.

[6] CyberSecurity Malaysia, *Digital Forensics – CyberCSI 2010 Annual Report,* http://www.cybersecurity.my/en/services/digital_forensics/about/main/detail/1987/index.html (May 2012).

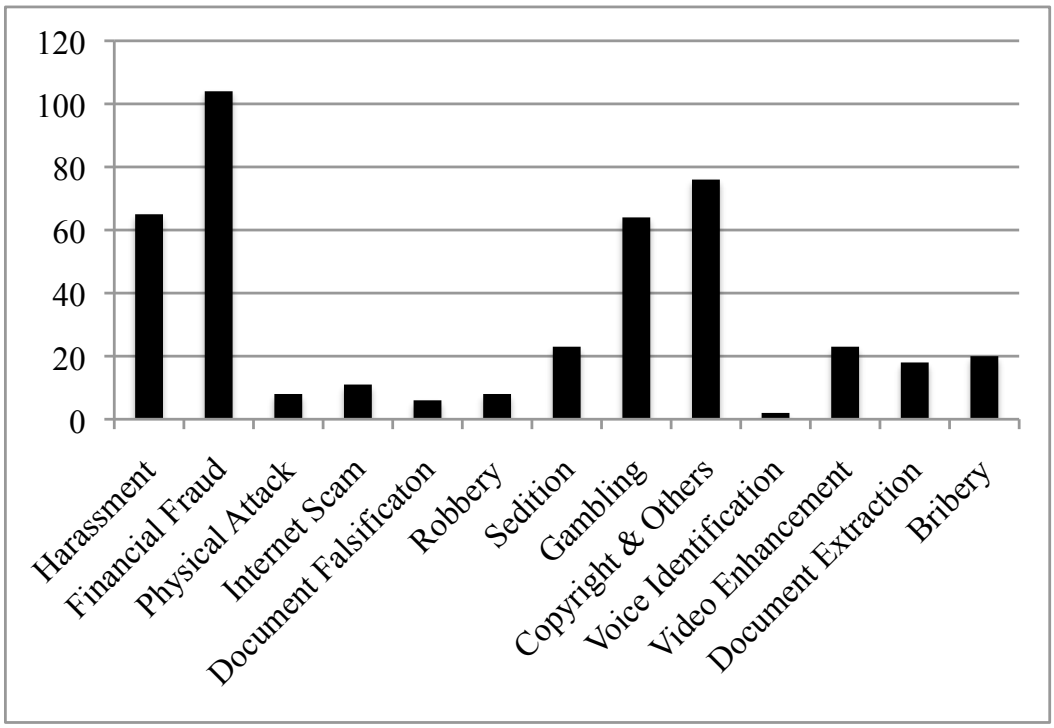

Figure 3. Cases by Categories

Examples of problems encountered in Malaysia [Heading type A]

It was challenging because case increased yearly. Analysis of diverse technologies was the main problem for DFD and still is. Some of 2010 cases were problematic and malfunctioned. It must be dealt with specialized techniques.

DVR recovery (DVRR) is an example and expertise in this subject is necessary because video based cases are increasing by approximately 15% annually. It is further justified when the government is installing more CCTVs[7].

If DVRR is failed, other forensic analyses such video authentication, image enhancement and identification could not be conducted. Its major problems are usually customized, proprietary and corrupted DVR with variety video file formats. Video file with timestamp extraction and playback are complicated in these circumstances. Using commercial and open source digital forensics tools are often ineffective.

[7] M. N. Anis, *176 CCTVs placed around Putrajaya to prevent crimes*, http://thestar.com.my/news/story.asp?file=/2010/8/10/nation/6825102&sec=nation (August 2010).

Digital forensics research in Malaysia [Heading type A]

Innovation is the answer to this sort of problem. DFD has a research unit to handle matter from the operational side. Hypothetically analyzing data streams and not file system can resolve the DVR complexity.

DVRR technique information and tool are not freely available. Existing research on it is limited and empirical examination is currently ongoing by DFD. Best practice guidelines and software tool will be developed to assist digital forensics analysts in their work. Nevertheless, a scientifically proven DVRR framework with three main steps is completed and can be referred below.

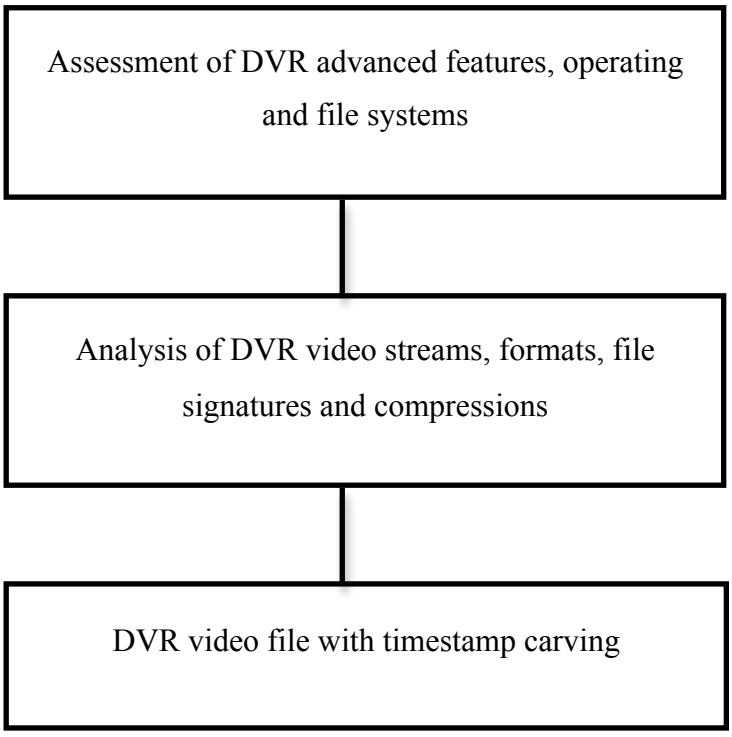

Figure 4. DVRR Framework

Digital forensics procedures in Malaysia [Heading type A]

DFD's standard operating procedures (SOP) in principle consist of identification, preservation, recovery, analysis and presentation of digital evidence. It is inline with ASCLD/LAB-International requirement, an American Society of Crime Laboratory Directors Laboratory Accreditation Board and ISO 17025 standard. This is simply to

assert high quality and trustworthy foundations[8]. The LEA values these trades and they are sending more evidences to be processed by DFD.

All operation analysts must adhere to the SOP strictly. It is from the first day they accept the evidence or during crime scene mission until the analysis is completed. This is to avoid any issue in the court of law as expert witness. Additionally, DVRR best practice guidelines that are going to be developed by DFD are recommended for reference when giving opinion evidence. This kind of document is scientifically produced.

DFD SOP also includes guidelines in giving expert witness testimony. They are: Understand the acts, Review validation of findings, Statement taking and legal standing, Prosecution approach, Presentation style, Court testimonial and cross examination and Post-mortem analysis.

Opinion of an expert witness is based on the facts in a case and must be proved by admissible evidence. This is on the ground that the courts need a computer expert 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 seen from Section 399 of the Criminal Procedure Code. CyberSecurity Malaysia digital forensics analyst report is recognized under the section 399(2)(f) of the Criminal Procedure Code Act 593. In the clause states any person or class of persons to whom the Minister by notification in the Gazette declares that the provisions of this section

[8] J. Slay, YC. Lin, B. Turnbull, J. Beckett, P. Lin, "Towards a Formalization of Digital Forensics," *The Advances in Digital Forensics V, IFIP Advances in Information and Communication Technology* (2009): vol. 306, pp. 37.

shall apply.

Digital forensics has been extensively consulted in Malaysia's court to inculpate or exculpate a suspect[9]. The court has accepted digital evidence and digital forensics expert is called to provide expert opinion. Eleven cases have been taken to the court under Section 211 and 233 of the Malaysian Communications and Multimedia Act (CMA) 1998[10]. The suspects are charged for posting coarse website comments, short message service (SMS) and e-mails that insult the Sultan of Perak (one of the states in Malaysia).

Digital forensics progress in Malaysia [Heading type A]

Malaysia government is supportive of DFD laboratory development. This is important because the cost is high. Careful planning on people, process and facilities are the success factor.

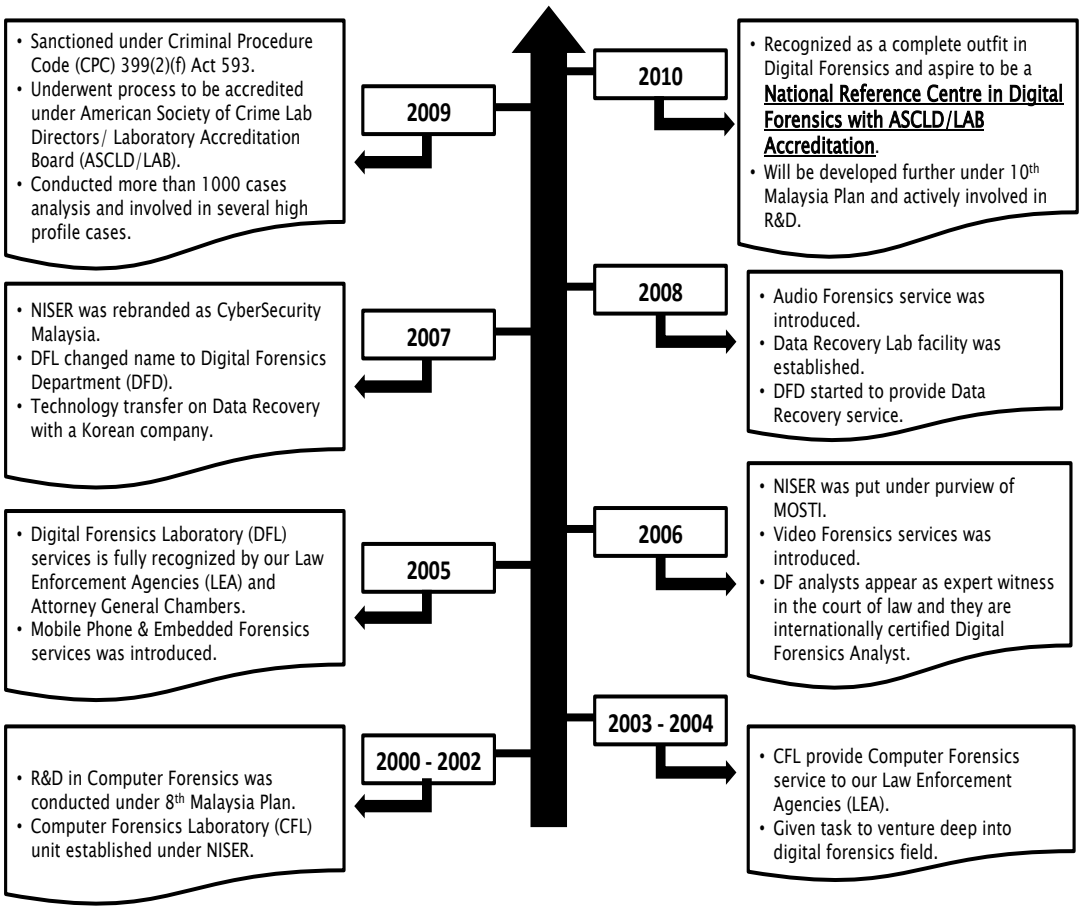

Figure 5. DFD Progress from 2000 to 2010

[9] Aswami A., Izwan I., "Digital Forensics in Malaysia," *The Digital Evidence and Electronic Signature Law Review* (October 2008): 161-165.
[10] J. A. Surin, *11 cases brought to court under CMA*, http://www.thenutgraph.com/eleven-cases-brought-to-court-under-cma/ (May 2012).

The progress must be in parallel that includes training, laboratory accreditation and installation of equipment (plus future expansion). Figure 5 summarizes the progress of DFD overall development from 2000-2010. As of 2011, DFD laboratory is ASCLD/LAB accredited.

Brief comparison with Japan and discussion [Heading type A]

Japan is committed on fighting cybercrime and cyber terrorism[11]. Cybercrime in Japan has risen since 2003. Fraud and fraud using the Internet were highest in 2007 with 1512 and 1229 cases respectively. The lowest was cybercrime of copyright with 165 cases in 2007.

Fraud case was common between Malaysia and Japan. It is alarming to note fraud case is rising. In fact the case increases every each year.

Many digital forensics outfits operate in silos. Perhaps it is due to the confidentiality nature of it. DFD has to initiate new efforts.

The DFD statistics are indicator that cases will be tougher. Cloud computing forensics is one big example. Operational cooperation is needed due to borderless nature of the crime. Moreover, it should be extended to research and development as well. This new endeavors can resolve challenging cases. Operational analyst does not have the time for research.

In a span of ten years, DFD proved successful. This job deals with fast evolving technologies and poses new threats. New plans must be devised in order to stay relevant.

One notable development in Japan is 'The Institute of Digital Forensics'. It is a non-profit organization looking into the area of technology development, globalization, legal reform, public awareness, civilian research and development and higher education in computer forensics. It is acting as the intermediary among stakeholders, government, national police agency, industry, education and promoting the development of digital forensics in Japan.

[11] J. Liu, T. Uehara, "Computer Forensics in Japan: A Preliminary," *The 2009 International Conference on Availability, Reliability and Security* (2010): pp. 1007-1011.

It is ideal to have DFIM similar to Japan. This noble idea is to maintain the progress of digital forensics. It is justifiable by looking at the contribution of DFD since 2000. With this trust and appointment, more programs can be delivered.

No	Program	Objective
1	Research and Development	• Conduct research based on operational or anticipated problems. • Outputs from research are turned into innovative process (technique) and product (tool). • Less dependence (independent) on commercial tools. • Capable of resolving own problem by sharing cases complexity between practitioner and researcher.
2	Globalization	• Able to work with counter part. • Ensure quality of service at par with others. • Collaboration can be initiated.
3	Legal Reform	• Better protection for digital forensics analyst. • New act specifically for digital crime.
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.
6	Cooperation	• Cooperation among digital forensics organizations in other countries by sharing general case information. • For cross border engagement to fight against cybercrime. • Cooperation can include research and development initiatives with the aim to reduce cost.
7	Others	• Better recognition for digital forensics analyst.

		• Centralized service with state of the art facilities. • Control environment with secured system to protect evidence.

Table 1. New Programs for DFIM

Conclusion and future work [Heading type A]

Digital forensics in Malaysia is not new and CyberSecurity Malaysia has been promoting digital forensics service since year 2000. The government of Malaysia has been supportive by providing operation and development funding. Cases are resolved and the monetary loss due to cases is reduced considerably.

As a way forward it timely to establish DFIM. It is to bring the service, capability and capacity to the next level. For future work, it is recommended that the DFIM programs to be detail up.